z/OS Communications Server

Shared Memory Communications - Direct Memory Access

Version 2 Release 2

Note:
Links to related publications are from original documents and might not work. The links to publications are included for reference purposes only.

Contents

Tables

Chapter 1. New Function Summary

V2R2 new function summary

Shared Memory Communications - Direct Memory Access

z/OS® V2R2 Communications Server provides significant performance improvements for TCP protocol workloads that are deployed on the same system Z CPC. This solution uses Shared Memory Communications - Direct Memory Access (SMC-D) for TCP connections to local peers which also support this function.

Incompatibilities: This function does not support IPAQENET and IPAQIDIO interfaces that are defined by using the DEVICE, LINK, and HOME statements. Convert your IPAQENET and IPAQIDIO definitions to use the INTERFACE statement to enable this support.

Dependencies:

- This function requires an IBM z13™ GA2 level of hardware.
- This function requires at least one Internal Shared Memory (ISM) device that is configured in the Hardware Configuration Definition (HCD).

To enable the SMC-D, complete the appropriate tasks in Table 1.

Table 1. Task topics to enable SMC-D

Task	Reference
If you are using IPv4 QDIO interfaces that are defined with the DEVICE, LINK, and HOME statements, and want to use SMC-D for traffic over these interfaces, convert those definitions to use the IPAQENET INTERFACE statement.	Steps for converting from IPv4 IPAQENET DEVICE, LINK, and HOME definitions to the IPv4 IPAQENET INTERFACE statement in z/OS Communications Server: IP Configuration Guide
If you are using IPv4 HiperSockets™ interfaces that are defined with the DEVICE, LINK, and HOME statements, and want to use SMC-D for traffic over these interfaces, convert those definitions to use the IPAQIDIO INTERFACE statement.	Steps for converting from IPv4 IPAQIDIO DEVICE, LINK, and HOME definitions to the IPv4 IPAQIDIO INTERFACE statement in z/OS Communications Server: IP Configuration Guide
Configure at least one ISM device in HCD.	*z/OS Hardware Configuration Definition (HCD) Reference Summary*
Select a unique physical network (PNet) ID for each of the networks. Configure the appropriate PNet ID in HCD for each OSD and/or IQD CHPID on a network and configure the PNet ID on the ISM device to be used on that network.	*z/OS Hardware Configuration Definition (HCD) Reference Summary*
Configure SMCD on the GLOBALCONFIG statement in the TCP/IP profile.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference

Table 1. Task topics to enable SMC-D (continued)

Task	Reference
For each IPv4 interface to be used for SMC-D, configure a nonzero subnet mask on the INTERFACE statement in the TCP/IP profile and use the same subnet value as the peer stack that resides on the same system Z CPC. For each IPv6 interface to be used for SMC-D, ensure that the interface has at least one associated prefix in common with the peer stack that resides on the same system Z CPC.	Shared Memory Communications in z/OS Communications Server: IP Configuration Guide
Optionally, restrict SMC from being used by certain server applications by coding the NOSMC option on the PORT or PORTRANGE statement that defines the server port.	PORT statement and PORTRANGE statement in z/OS Communications Server: IP Configuration Reference
Display whether the stack is enabled for SMC-D by issuing the Netstat CONFIG/-f command.	Netstat: CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display the status of the ISM PFIDs.	D PCIE command in z/OS MVS System Commands
Display information about the dynamic ISM TRLEs by issuing the D NET,ID=*trle*, or D NET,TRL,TRLE=*trle* command.	DISPLAY ID command and DISPLAY TRL command in z/OS Communications Server: SNA Operation
Display information about an ISM interface by issuing the Netstat DEvlinks/-d command for the ISM interface.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display the PNet ID for an active OSD, IQD, or ISM interface using the netstat DEvlinks /-d command or by issuing the D NET,ID=trle or D NET,TRL,TRLE=*trle* command.	See the following topics: • DISPLAY ID command and DISPLAY TRL command in z/OS Communications Server: SNA Operation • Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display information about the number of sends, receives, and bytes that went over an ISM interface by issuing the Netstat DEvlinks/-d command for the ISM interface.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display how many TCP connections are using SMC-D by issuing the Netstat STATS/-S command.	Netstat STATS /-S report in z/OS Communications Server: IP System Administrator's Commands
Display information about storage that is being used by TCP/IP for SMC-D by issuing the D TCPIP,,STOR command.	D TCPIP,,STOR command in z/OS Communications Server: IP System Administrator's Commands
Display information about SMC-D links by issuing the Netstat DEvlinks/-d command with the SMC parameter.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display information about interfaces by issuing the Netstat DEvlinks/-d command using the PNETID modifier.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands

To find all new and updated topics about Shared Memory Communications - Direct Memory Access, see Table 2.

Table 2. All new and updated topics about Shared Memory Communications - Direct Memory Access

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• Shared Memory Communications

Table 2. All new and updated topics about Shared Memory Communications - Direct Memory Access (continued)

Book name	Topics
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement • INTERFACE - IPAQENET OSA-Express® QDIO interfaces statement • INTERFACE - IPAQIDIO HiperSockets interfaces statement • INTERFACE - IPAQENET6 OSA-Express QDIO interfaces statement • INTERFACE - IPAQIDIO6 HiperSockets interfaces statement • IPCONFIG statement • IPCONFIG6 statement • PORT statement • PORTRANGE statement
z/OS Communications Server: IP Programmer's Guide and Reference	• TCP/IP callable NMI (EZBNMIFR) • EZBNMIFR: Poll-type requests • Format and details for poll-type requests • Filter request section • TCP/IP NMI response format • TCP/IP profile event record (subtype 4) • TCP/IP profile record IPv4 configuration section • TCP/IP profile record IPv6 configuration section • TCP/IP profile record Global configuration section • TCP/IP profile record interface section
z/OS Communications Server: IP Diagnosis Guide	• OPTIONS keywords • Diagnosing problems with Shared Memory Communications
z/OS Communications Server: IP System Administrator's Commands	• DISPLAY TCPIP,,NETSTAT • D TCPIP,,STOR command • The TSO NETSTAT command syntax • The z/OS UNIX netstat command syntax • The Netstat command filter • Netstat ALL/-A report • Netstat ALLConn/-a report • Netstat: CONFIG/-f report • Netstat COnn/-c report • Netstat DEvlinks/-d report • Netstat HElp/-? report • Netstat PORTList/-o report • Netstat STATS /-S report • z/OS UNIX and TSO Netstat option comparison
z/OS Communications Server: IP and SNA Codes	• Data link control (DLC) status codes

Table 2. All new and updated topics about Shared Memory Communications - Direct Memory Access (continued)

Book name	Topics
z/OS Communications Server: SNA Operation	• DISPLAY ID command • DISPLAY INOPDUMP command • DISPLAY TRL command • DISPLAY VTAMOPTS command • MODIFY INOPDUMP command • MODIFY TNSTAT command • MODIFY TRACE command • MODIFY VTAMOPTS command • START command
z/OS Communications Server: SNA Network Implementation Guide	• Resources automatically activated by VTAM® • Gathering tuning statistics
z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures	• I/O trace
z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT	• Trace options for the VIT • AFSM entry for altering an FSM state • ICR entry for a control register operation • ICR2 entry for a control register operation (part 2) • ICR3 entry for a control register operation (part 3) • IOSP entry for invoking a Peripheral Component Interconnect Express (PCIe) service (Part 1) • IOS2 entry for invoking a Peripheral Component Interconnect Express (PCIe) service (Part 2) • IOS3 entry for invoking a Peripheral Component Interconnect Express (PCIe) service (Part 3) • IPLx entry for an internal shared memory (ISM) polling operation • IPLA entry for an internal shared memory (ISM) polling operation (part 2) • ISPx entry for invoking an Internal Shared Memory (ISM) Verb (part 1) • ISP2 entry for invoking an Internal Shared Memory (ISM) Verb (part 2) • ISP3 entry for invoking an Internal Shared Memory (ISM) Verb (part 3) • IUTX mapping and field descriptions • IUT6 mapping and field descriptions • PCIx entry for program-controlled or suspend interrupt • PCIR mapping and field descriptions • QSRB entry for Queue Service Request Block (SRB) event • RPST entry for invoking a RoCE Post command (Part 1) • RPSA entry for invoking a RoCE Post command (Part 3)

Table 2. All new and updated topics about Shared Memory Communications - Direct Memory Access (continued)

Book name	Topics
z/OS Communications Server: SNA Resource Definition Reference	• Start options syntax diagrams • AIMON start option • INOPDUMP start option
z/OS Communications Server: Quick Reference	• D TRL command • F VTAMOPTS command • Start options
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	• EZZ0378I • EZZ0839I • EZZ8453I
z/OS Communications Server: SNA Messages	• IST087I • IST1221I • IST1314I • IST1451I • IST1717I • IST1865I • IST1904I • IST2337I • IST2390I • IST2391I • IST2392I • IST2393I • IST2407I • IST2409I • IST2411I • IST2417I • IST2418I • IST2419I • IST2420I • IST2421I • IST2422I • IST2423I
z/OS Summary of Message and Interface Changes	• PROFILE.TCPIP statement and parameter changes • Netstat operator commands (DISPLAY TCPIP,,NETSTAT) • General updates of IP operator commands • NETSTAT TSO commands • Netstat UNIX commands • TCP/IP callable NMI (EZBNMIFR) • TCP/IP stack records • SNA start options behavior changes • SNA commands • SNA command behavior changes • VTAM internal trace entries
z/OS MVS System Commands	• D PCIE command

Chapter 2. IP Configuration Guide

Shared Memory Communications

Shared Memory Communications (SMC) enables two SMC capable peers to communicate by using memory buffers that each peer allocates for the partner's use. There are two types of Shared Memory Communications:

- Shared Memory Communications over Remote Direct Memory Access (SMC-R)
- Shared Memory Communications - Direct Memory Access (SMC-D)

SMC improves throughput, lowers latency and cost, and maintains existing functions. You do not need to change resources, such as host names and IP addresses, because you can use existing IP topology and addressing to identify virtual servers. You do not need to modify applications to use SMC to gain the performance benefits of communication by using SMC. Existing functions are preserved when SMC is used, such as the following functions:

- Load balancing, for example, sysplex distribution
- IP security zones
- Connection level security

Shared Memory Communications over Remote Direct Memory Access

Shared Memory Communications over Remote Direct Memory Access (RDMA), or Shared Memory Communications over RDMA (SMC-R), is a protocol solution that is based on sockets over RDMA. SMC-R enables TCP sockets applications to transparently use RDMA, which enables direct, high-speed, low-latency, memory-to-memory (peer-to-peer) communications. Communicating peers such as TCP/IP stacks dynamically learn about the shared memory capability by using traditional TCP/IP connection establishment flows, enabling the TCP/IP stacks to switch from TCP network flows to more optimized direct memory access flows that use RDMA.

RDMA is available on standard Ethernet-based networks by using the industry (InfiniBand Trade Association) standard referred to as RDMA over Converged Ethernet (RoCE). RoCE enables the use of both standard TCP/IP and RDMA solutions such as SMC-R over the same physical LAN fabric. SMC-R requires the IBM® 10GbE RoCE Express feature, which is sometimes referred to as an RDMA network interface card (RNIC). SMC-R provides an enterprise class of services for RDMA that are designed for IBM enterprise class data center networks.

As shown in Figure 1 on page 8, SMC-R enables two virtual servers that support RoCE to logically share memory through the IBM 10GbE RoCE Express feature (shown as RNIC in Figure 1 on page 8) and over the RoCE network. When a virtual server that supports RoCE detects that a remote TCP connection partner supports shared memory communications, the connection is transparently and dynamically switched to use SMC-R protocols. The applications are unaware of the use of shared memory for communications.

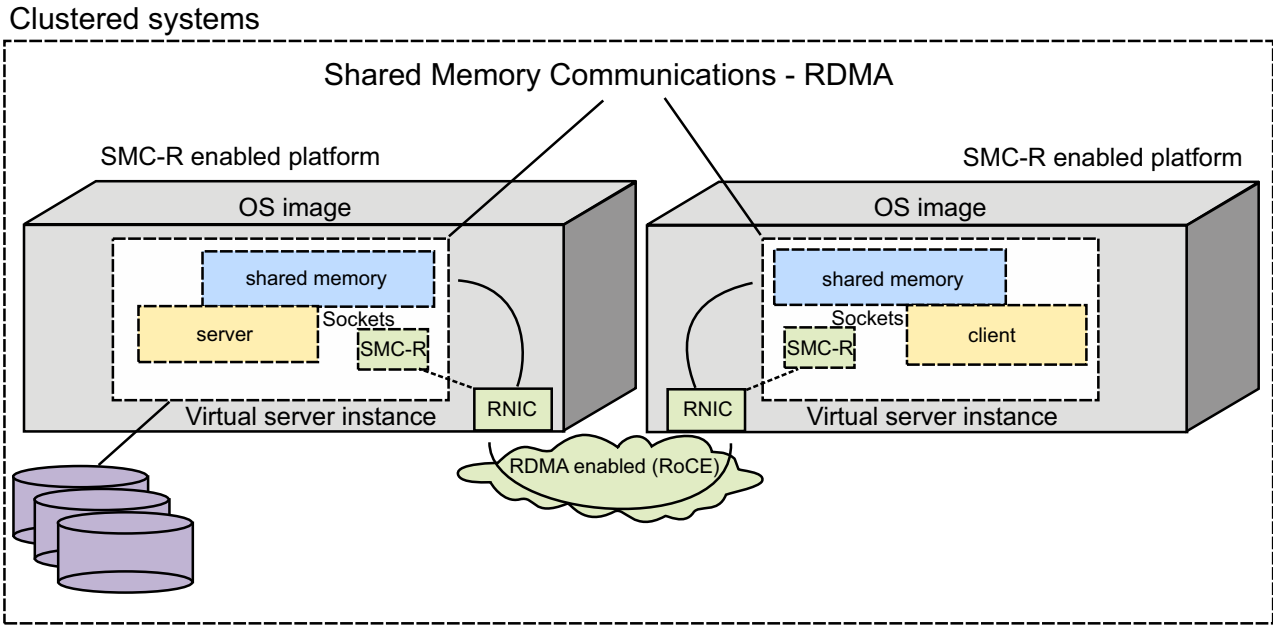


Figure 1. Shared Memory Communications over RDMA (SMC-R)

When redundant IBM 10GbE RoCE Express interfaces are provisioned, SMC-R also transparently provides the capability for failover processing when a failure is detected with SMC-R communications.

Remote Direct Memory Access over Converged Ethernet

Remote Direct Memory Access (RDMA) enables a host to make a subset of its memory directly available to a remote host. After RDMA connectivity is established between two TCP/IP stacks, either host can write to the memory of the remote host with no involvement from the remote host processors or operating system. RDMA enables efficient communications between the hosts because all the low-level functions are managed by RDMA network interface cards (RNICs) that are connected to each host, rather than by the software stack as is normally done for TCP/IP communications.

RDMA was traditionally confined to high-performance computing (HPC) environments where the cost of maintaining RDMA-capable network fabrics such as InfiniBand was justified given the emphasis of performance over cost. Now that RDMA is available on Ethernet fabrics through standards such as RDMA over Converged Ethernet (RoCE), the cost of adopting RDMA is lower because it can be enabled on the existing Ethernet fabrics that are used for IP network communications. Standard Ethernet management techniques are used to configure the RNIC adapters.

z/OS Communications Server provides support for sockets over RDMA by using SMC-R protocols. VTAM device drivers use Peripheral Component Interconnect Express (PCIe) operations to manage IBM 10GbE RoCE Express features that are defined to z/OS. Up to 16 10GbE RoCE Express PFID values can be defined to a z/OS TCP/IP stack.

Comparing 10GbE RoCE Express feature environments

An IBM 10GbE RoCE Express feature operates in either a dedicated or a shared RoCE environment.

z/OS Communications Server dynamically determines the operating environment supported by this generation of System z® when the first 10GbE RoCE Express feature is activated. Any additional RoCE Express features that are activated operate in the same environment that is determined when the first feature is activated.

Dedicated RoCE environment:

In a dedicated RoCE environment, z/OS Communications Server uses PCIe Physical Function services to manage the RoCE Express feature.

A RoCE Express feature operating in a dedicated RoCE environment can only be used by a single LPAR. z/OS allows the feature to be shared by up to eight TCP/IP stacks within a single LPAR. Each TCP/IP stack uses the same PCIe function ID (PFID) value to define its representation of the RoCE Express feature. The PFID value is defined by using traditional hardware configuration definition (HCD) tools. In a dedicated RoCE environment, only one of the two available ports can be used at a time.

Figure 2 on page 10 is an example of a 10GbE RoCE Express feature that is defined in a dedicated RoCE environment. A single z/OS image (z/OS 2) is using the 10GbE RoCE Express features identified by PCHID values 100 and 200. Two PFID values (0001 and 0016) are defined to represent the features, and the PFID values correspond to the FID values defined in the HCD for the features. No other z/OS images can use these two features, although up to eight stacks on z/OS 2 can use the features. In this example, port 1 is used on both features, and port 2 cannot be used when port 1 is in use.

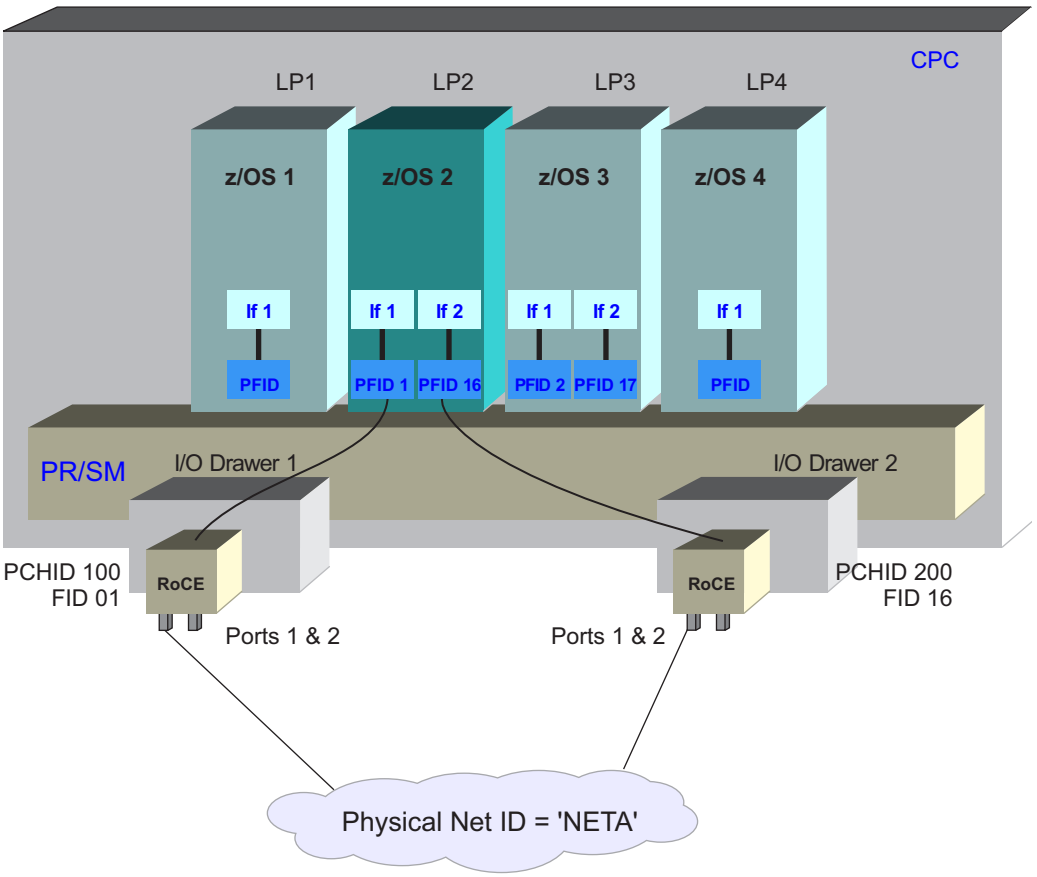


Figure 2. 10GbE RoCE Express feature in a dedicated RoCE environment

A dedicated RoCE environment mode is supported on an IBM zEnterprise® EC12 (zEC12) with driver 15, or an IBM zEnterprise BC12 (zBC12).

Shared RoCE environment:

In a shared RoCE environment, z/OS Communications Server uses PCIe Virtual Function (VF) services to manage the RoCE Express feature, and System z provides the Physical Function management.

A RoCE Express feature operating in a shared RoCE environment can be shared by up to 31 operating system instances or TCP/IP stacks across the same central processor complex (CPC). Each TCP/IP stack within an LPAR, or each operating system instance, uses a unique FID value to define its representation of the RoCE Express feature. These FID values are defined by using HCD tools. In the shared environment, both RoCE ports can be used at the same time.

Guideline: For a TCP/IP stack, the FID value is represented by a PFID value on the GLOBALCONFIG statement in the TCP/IP profile. In addition, the same or different TCP/IP stacks can share the two RoCE Express ports of an individual RoCE Express feature if different PFID values are configured for the individual ports.

Figure 3 on page 11 is an example of a 10GbE RoCE Express feature operating in a shared RoCE environment. Two z/OS images are using the 10GbE RoCE Express features identified by PCHID values 100 and 200. Four unique PFID values are defined, two per z/OS image, to represent the usage of the features. The PFID

values correspond to the FID values defined for the features in the HCD. In this example, the combination of PFID and port is unique for all four interfaces, but TCP/IP stacks are sharing the same feature and port.

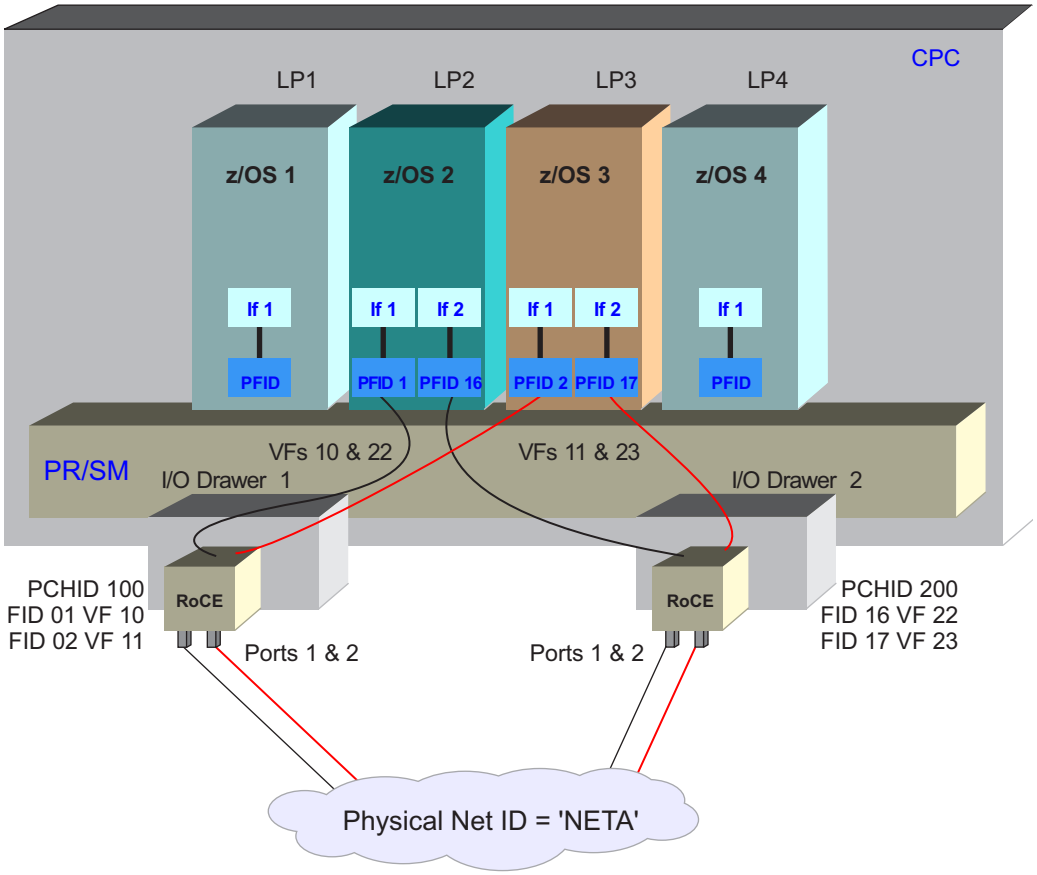


Figure 3. 10GbE RoCE Express feature in a shared RoCE environment

Guideline: For full redundancy at a TCP/IP stack, configure PFID values that are associated with physically separate 10GbE RoCE Express features. For example, in Figure 3, for z/OS 2, the two features are in different System z I/O drawers. Therefore, the failure of one I/O drawer or one feature does not affect the other I/O drawer or feature.

A shared RoCE environment must be used on the IBM z13™ (z13) or later systems.

Shared Memory Communications - Direct Memory Access

Shared Memory Communications - Direct Memory Access (SMC-D) uses internal shared memory (ISM) for communication between two SMC capable peers that are located on the same central processor complex (CPC). The communicating peers, such as TCP/IP stacks, dynamically detect the shared memory capability by using traditional TCP/IP connection establishment flows. The shared memory enables the TCP/IP stacks to switch from TCP network flows to more optimized direct memory access flows that use ISM.

As shown in Figure 4 on page 12, SMC-D enables two virtual servers that support ISM to logically share memory. When a virtual server that supports ISM detects that a TCP connection partner also supports shared memory communications by using ISM, the connection is transparently and dynamically switched to use

SMC-D protocols. The applications are unaware of the use of shared memory for communications.

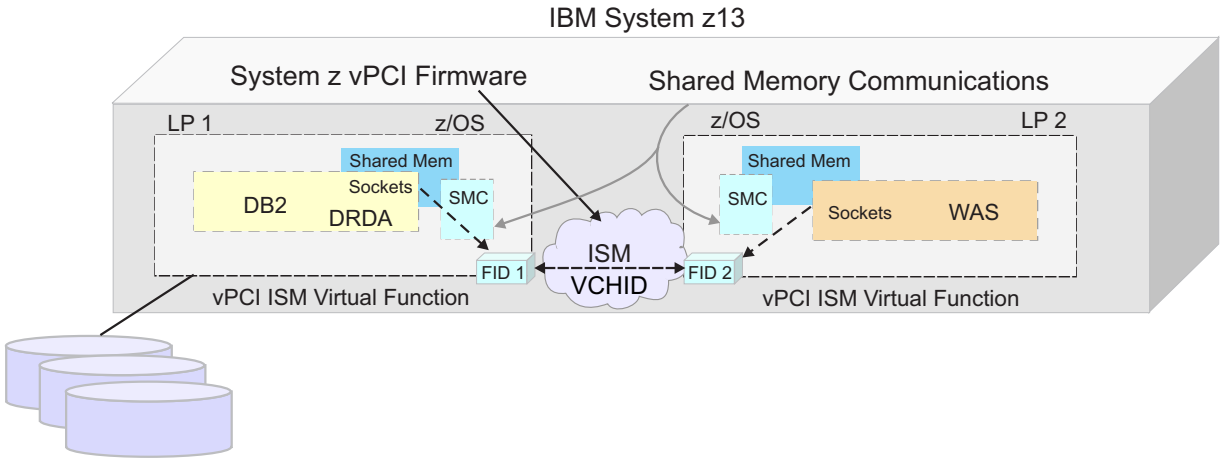


Figure 4. Shared Memory Communications - Direct Memory Access (SMC-D)

Shared Memory Communications terms

The following terms apply to Shared Memory Communications (SMC). You can use this list as needed for brief descriptions when you are using other SMC information.

Associated ISM interface
An internal shared memory (ISM) interface that is associated with an Shared Memory Communications - Direct Memory Access (SMC-D) capable interface that has the same physical network ID.

Associated RNIC interface
An IBM 10GbE RoCE Express interface that is associated with an Shared Memory Communications over Remote Direct Memory (SMC-R) capable interface that has the same physical network ID.

Direct memory buffer (DMB)
Local memory that is used to receive inbound data over an SMC-D link. The remote peer places TCP socket application data directly into the DMB that the local peer assigns to receive data for the TCP connection. The local peer then copies the data from the DMB into the receive buffer of the receiving socket application.

DMB element (DMBE)
The portion of a DMB that is associated with a specific TCP connection. Each DMB is partitioned into one or more DMBEs.

IBM 10GbE RoCE Express feature
A feature that enables Remote Direct Memory Access by managing low-level functions that the TCP/IP stack typically handles.

IBM 10GbE RoCE Express interface
An interface that is dynamically created by TCP/IP that uses a particular port of an IBM 10GbE RoCE Express feature.

Internal path
The System z internal PCIe infrastructure for IBM 10GbE RoCE Express

features. The internal path of a 10GbE RoCE Express feature is determined based on how the feature is plugged into the System z I/O drawers.

ISM device
The System z firmware that facilitates the use of internal shared memory for SMC-D processing. An ISM device is identified by a unique PCIe function ID (PFID) and a virtual channel ID (VCHID). An ISM device is configured in the hardware configuration definition (HCD) and is associated with a single physical network ID.

ISM interface
An interface that is dynamically created by TCP/IP to represent an ISM device for SMC-D capable interfaces with the same physical network ID.

Operating system images
Logical partitions (LPARs) or guest virtual machines that operate in the same central processor complex (CPC).

Physical channel ID (PCHID)
A 2-byte hexadecimal value that is used to uniquely define a RoCE Express feature.

PCIe function ID (PFID)

A value that represents the SMC device.

For SMC-R, the PFID value is configured on the SMCR parameter of the GLOBALCONFIG statement in the TCP/IP profile to identify an IBM 10GbE RoCE Express feature. The PFID represents a physical RoCE Express feature and must match a FID value configured in the hardware configuration definition (HCD) for the PCHID value that identifies the feature. When the RoCE Express feature is installed on a System z that supports a shared RoCE environment, the same physical feature can be shared with other operating system images, and multiple PFID values specified on the same GLOBALCONFIG statement can represent different ports on the same physical RoCE Express feature.

For SMC-D, the PFID value is obtained during ISM interface activation that identifies an ISM device. The PFID value matches an FID value that is configured in the HCD for the VCHID value that represents the ISM device.

Peripheral Component Interconnect Express (PCI Express, or PCIe)
A local bus that provides the high-speed data path between the processor and an SMC device. For SMC-R, the device is an attached IBM 10GbE RoCE Express feature. For SMC-D, the device is the ISM device.

Physical network ID (PNetID)
A value that is defined to uniquely identify your physical layer 2 LAN fabric or physical broadcast domain. You can use this value to logically associate the System z features, adapters, and ports to be physically connected to your network. You specify the PNetID in a single step within the hardware configuration definition (HCD), and all operating systems of all associated central processor complexes (CPCs) can dynamically learn and use this definition.

RDMA network interface card (RNIC)
An IBM 10GbE RoCE Express feature that enables Remote Direct Memory Access by managing low-level functions that are typically handled by the TCP/IP stack.

RDMA over Converged Ethernet (RoCE)
An InfiniBand Trade Association (IBTA) standard that enables Remote Direct Memory Access over Converged Ethernet.

Redundancy level
For an SMC-R link group, this value indicates the level to which z/OS Communications Server can provide dynamic failover processing if there is a failure of an underlying IBM 10GbE RoCE Express interface or the associated network hardware.

Reliable connected queue pair (RC QP)
A logical connection between two virtual servers that enables that specific pair of servers to use RDMA communications between themselves.

Remote Direct Memory Access (RDMA)
A high-speed, low-latency network communications protocol in which data is transferred directly to the memory of a remote host with no involvement from the remote host processors or operating system.

Remote memory buffer (RMB)
Local memory that is used to receive inbound data over an SMC-R link. The remote peer places TCP socket application data directly into the RMB that the local peer assigns to receive data for the TCP connection. The local peer then copies the data from the RMB into the receive buffer of the receiving socket application.

Rendezvous processing
The sequence of TCP connection management flows that are required to establish SMC communications between two peers.

RMB element (RMBE)
The specific portion of an RMB that is associated with a specific TCP connection. Each RMB is partitioned into RMBEs.

RoCE environments
Depending on the level of hardware that is used, the 10GbE RoCE Express feature operates in either a shared or a dedicated RoCE environment.

Dedicated RoCE environment
A dedicated RoCE environment applies to an IBM zEnterprise EC12 (zEC12) with driver 15, or an IBM zEnterprise BC12 (zBC12). In this environment, only a single operating system instance can use a physical RoCE feature. Multiple operating system instances cannot concurrently share the feature.

Shared RoCE environment
A shared RoCE environment applies to an IBM z13 (z13) or later system. In this environment, multiple operating system instances can concurrently use or share the same physical RoCE feature. With IBM z13 (z13) or later systems, the RoCE Express feature operates in a shared environment even if only one operating system instance is configured to use the feature.

SMC-D link
A logical representation of communication between two virtual servers that use SMC-D protocols. The concept of an SMC-D link exists primarily for operational consistency with SMC-R processing.

SMC-R link
A logical point-to-point link between two virtual servers that is used for SMC-R communications.

SMC-R link group
A logical grouping of equal SMC-R links between two communicating peers.

Staging buffer
Memory that the TCP/IP stack allocates for outbound SMC-R data. Staging buffers are not associated with specific SMC-R links or link groups, and are used by all TCP connections that traverse SMC-R links on this stack. Only local applications access the staging buffer storage.

Virtual channel ID (VCHID)
A 2-byte hexadecimal value that is used to uniquely define an ISM device.

Shared Memory Communications concepts

The following concepts apply to Shared Memory Communications (SMC).

Rendezvous processing

Shared Memory Communications (SMC) is enabled by using the GLOBALCONFIG statement in the TCP/IP profile data set.

- Shared Memory Communications over RDMA (SMC-R) is enabled by specifying one or more Peripheral Component Interconnect Express (PCIe) function ID (PFID) values on the SMCR parameter of the GLOBALCONFIG statement in the TCP/IP profile data set. Each PFID value represents an IBM 10GbE RoCE Express feature that is configured by using the traditional hardware configuration definition (HCD) tools. TCP/IP activates 10GbE RoCE Express interfaces when the first SMC-R capable interface is started. SMC-R capable interfaces include IPAQENET or IPAQENET6 interfaces with the OSD channel path ID type. Any TCP connections that are routed over SMC-R capable interfaces are eligible for SMC-R communications.
- Shared Memory Communications - Direct Memory Access (SMC-D) is enabled by specifying the SMCD parameter of the GLOBALCONFIG statement in the TCP/IP profile data set. When SMC-D capable interfaces are activated, z/OS Communications Server selects an available ISM device that is associated with the same physical network as the SMC-D capable interface. Only one ISM device is activated for each physical network. The ISM device is represented by a Peripheral Component Interconnect Express® (PCIe) function ID (PFID) value that is configured by using the traditional hardware configuration definition (HCD) tools. SMC-D capable interfaces include IPAQENET or IPAQENET6 interfaces with the OSD channel path ID type, and IPAQIDIO and IPAQIDIO6 HiperSockets interfaces. Any TCP connections that are routed over SMC-D capable interfaces are eligible for SMC-D communications.

The decision about whether an eligible connection uses SMC communications is reached during traditional TCP connection establishment. *Rendezvous processing* is the term that is used to describe the sequence of connection management flows (shown in Figure 5 on page 16) that are required to establish SMC-R communications between two peers.

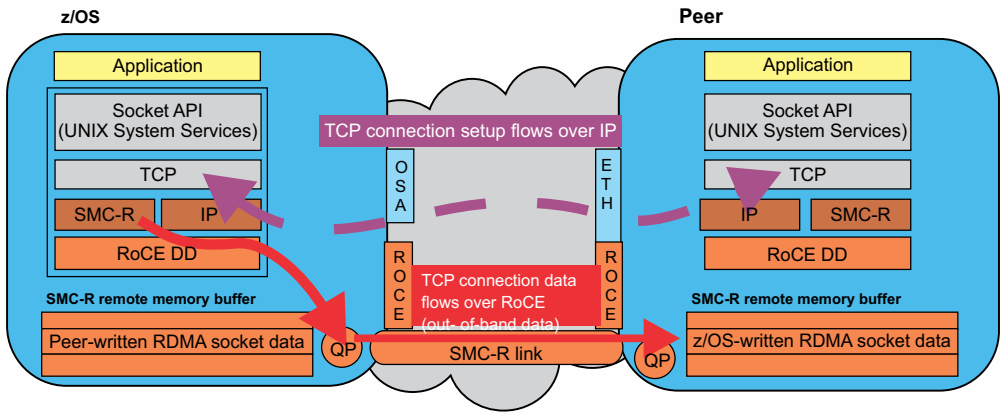


Figure 5. Rendezvous processing

The exchange of information occurs in different stages:

- Extra information in TCP connection establishment flows

  Applications still use the standard three-way handshake mechanisms to establish TCP connections. When SMC-R or SMC-D communications are enabled, the client and the server can indicate support for either SMC-R or SMC-D protocols:

  – The client adds TCP options settings in the SYN request to indicate which protocols that the client supports.

  – The server responds with TCP options settings in the SYN-ACK response to indicate which protocols that the server supports.

  No additional exchange of information is required in this stage of the rendezvous processing.

- In-band SMC Connection Layer Control (CLC) messages

  Conceptually, CLC messages are similar to the SSL handshake processing that occurs after the TCP connection is established.

  SMC-D protocols are preferred over SMC-R protocols. If both the client and the server indicate support for SMC-D processing, after the TCP connection is established, the client and the server negotiate the use of SMC-D for this TCP connection by using SMC-D CLC messages that flow as in-band data over the TCP connection.

  The SMC-D CLC messages exchange the following information:

  – Peer identification information

  – SMC-D buffer information that is necessary to exchange data between the peers

  For detailed description about the information that SMC-D CLC messages exchange, see “SMC-D links” on page 21.

  If the attempt to establish SMC-D communications succeeds, the SMC-D link is established, and the peers can start exchanging data by using the SMC-D buffers.

  If the attempt to establish SMC-D communications fails and both the client and the server indicate support for SMC-R processing, the client and the server negotiate the use of SMC-R for this TCP connection by using SMC-R CLC messages that flow as in-band data over the TCP connection.

  The SMC-R CLC messages exchange the following information:

  – Network routing information

  – RDMA over Converged Ethernet (RoCE) routing credentials

  - SMC-R buffer information that is necessary to select or establish the RoCE path between the peers

  For detailed description about the information that SMC-R CLC messages exchange, see "SMC-R links" on page 18.
- SMC-R Link Layer Control (LLC) messages

  After the SMC-R information is exchanged, SMC-R LLC messages are exchanged across the RoCE fabric to confirm that the RoCE information is correct and that the remote memory can be accessed. This stage is skipped if an existing RoCE connection is used for this TCP connection.

The TCP/IP stack does not allow the client and server applications to exchange application data during rendezvous processing. Because no application data is exchanged, the TCP connection can revert to IP protocols if there is a failure during the setup of the SMC communications. However, after the TCP connection is committed to using SMC protocols, the TCP connection cannot fall back to using IP protocols if SMC communications encounter an error.

- For SMC-R communications, the TCP connection is committed to use SMC logic after the RoCE connection is confirmed by using the SMC-R LLC messages.
- For SMC-D communications, the TCP connection is committed to use SMC logic after the successful exchange of SMC-D CLC messages.

Both the client and the server nodes maintain a series of rendezvous timers to ensure that the rendezvous processing completes in time. If one of the timed events does not complete as expected, the TCP connection reverts to using IP protocols. However, future TCP connections can still attempt to use SMC.

To reduce the overhead of persistent rendezvous failures (TCP connections reverting to using IP protocols) to the same destination IP address, you can use the default AUTOCACHE function. This function is controlled by the AUTOCACHE and NOAUTOCACHE subparameters of the SMCGLOBAL parameter on the GLOBALCONFIG profile statement and is set to AUTOCACHE by default. The AUTOCACHE function caches rendezvous failures per IP address destination. If the AUTOCACHE function detects too many rendezvous failures to a specific IP address, the function prevents additional rendezvous attempts to that IP address. The AUTOCACHE function is started only when you enable SMC. For more information about enabling SMC, see the description of the GLOBALCONFIG SMCR and SMCD parameters in z/OS Communications Server: IP Configuration Reference.

Even though the data is sent out of band with SMC communications, the TCP connection remains active, primarily to facilitate connection termination processing. If you have TCP server applications that primarily use many short-lived TCP connections, you might want to avoid rendezvous processing. You can prevent these server applications from using SMC in one of the following ways:

Use the AUTOSMC monitoring function

The AUTOSMC monitoring function dynamically monitors incoming TCP connections to local TCP server applications and determines whether the use of SMC is beneficial for the workload. This function is configured by the AUTOSMC and NOAUTOSMC subparameters of the SMCGLOBAL parameter on the GLOBALCONFIG profile statement and is set to AUTOSMC by default. However, the AUTOSMC monitoring function is started only when you enable SMC. For more information about enabling SMC, see the description of the GLOBALCONFIG SMCR and SMCD parameters in z/OS Communications Server: IP Configuration Reference. If

the function determines that most of the incoming connections are short-lived and exchange a small amount of data then SMC processing will be bypassed for all new connections to this server. This monitoring is dynamic in nature so that it can detect changes in workload patterns. You can monitor the results of this dynamic monitoring and SMC enablement/disablement using the Netstat ALL/-A command. For more information about the Netstat ALL/-A command, see z/OS Communications Server: IP System Administrator's Commands.

Disable SMC eligiblity for the port
Explicitly specify the NOSMC parameter on the PORT or PORTRANGE statements that define the port or ports that the server application uses. For more information, see z/OS Communications Server: IP Configuration Reference.

Shared Memory Communications links and link groups

After two Shared Memory Communications (SMC) peers recognize during rendezvous processing that shared memory communications are possible, the peers create SMC links and, in the case of SMC-R, SMC link groups.

SMC-R links: After two Shared Memory Communications over RDMA (SMC-R) peers recognize during rendezvous processing that shared memory communications are possible, a logical point-to-point SMC-R link is established between the stacks over the RDMA over Converged Ethernet (RoCE) fabric. An SMC-R link, as shown in Figure 6 on page 19, is uniquely defined by a combination of the following information:

- Remote and local virtual MAC (VMAC) values

  A VMAC is a 6-byte value that is a virtual representation of the physical MAC address for an IBM 10GbE RoCE Express interface (shown as RNIC in Figure 6 on page 19).

  Each TCP/IP stack that activates a particular 10GbE RoCE Express interface is assigned a different VMAC value.
- Remote and local global ID (GID) values

  A GID is a 16-byte value. z/OS Communications Server generates the GID values by converting the VMAC address of the 10GbE RoCE Express interface into an IPv6 link-local address.
- Remote and local queue pair (QP) values

  A QP represents one end of the logical connection between two RDMA peers. A combination of two reliable connected queue pairs (RC QPs) forms a single logical point-to-point link. The link enables exactly one pair of communicating RDMA peers to send and receive messages and initiate RDMA activities between themselves. A 10GbE RoCE Express interface associates units of work, such as confirmation of sent data or indication of received data, to a specific QP to enable the SMC-R protocols to identify which TCP/IP stack to notify for the unit of work. The stack then determines which TCP connection that uses that RC QP is to process the data.
- Virtual LAN (VLAN) ID

  You can optionally use VLANs to isolate application traffic into different virtual networks on the same physical Ethernet.

  – If you use VLANs, the VLAN ID specified on the IPAQENET or IPAQENET6 INTERFACE statement is used as an attribute to create unique SMC-R links between the peers for unique VLANs. In other words, the SMC-R links are VLAN qualified.

– If you do not use VLANs, no VLAN ID is used to define the SMC-R links between the peers. In other words, the SMC-R links are not VLAN qualified.

For more information about using VLANs, see "SMC-R VLANID usage" on page 25.

Application traffic between the two peers that uses the same remote and local VMACs, GIDs, and QPs, and that is associated with the same VLAN when VLANs are defined, can use the same SMC-R link.

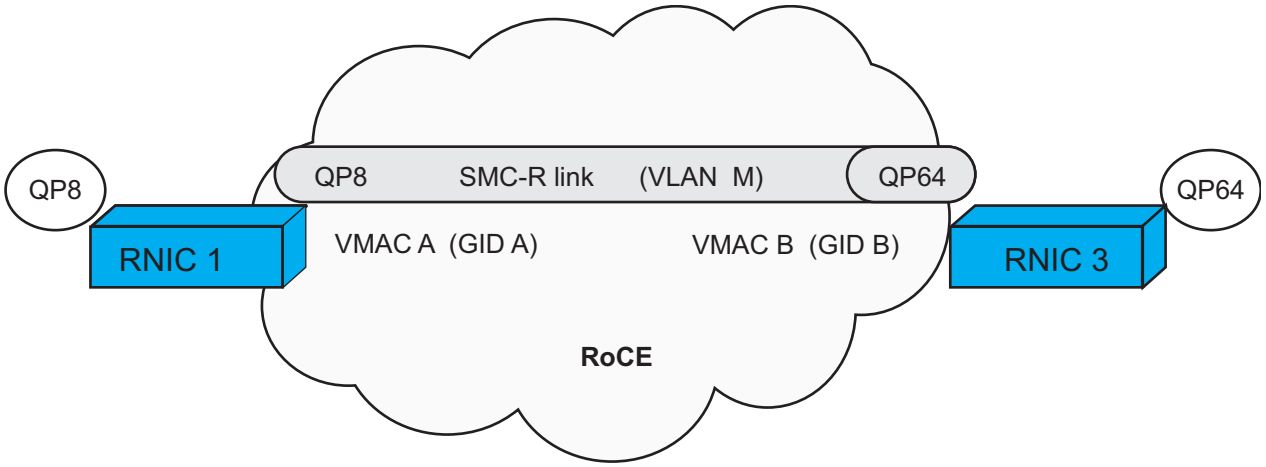


Figure 6. Identifying an SMC-R link

In addition to the 7-tuple (local VMAC, GID, QP# + remote VMAC, GID, QP# + VLAN ID) that uniquely defines an SMC-R link, each peer assigns a 4-byte SMC-R link ID value that uniquely identifies the SMC-R link within its own resource space. This SMC-R link ID is exchanged between peers and is intended to be used for network management and diagnostic purposes. For instance, you can use the SMC-R link ID to filter Netstat report information that is related to a specific SMC-R link. For more information, see "Displaying SMC information" on page 48.

An SMC-R link supports multiple TCP connections between the same two peers, as shown in Figure 7 on page 20. The first TCP connection between the peers establishes the SMC-R link, and subsequent TCP connections between the peers can use the previously established link. Because subsequent TCP connections between the peers can use the previously established link, extra SMC-R link setup costs between the peers are avoided.

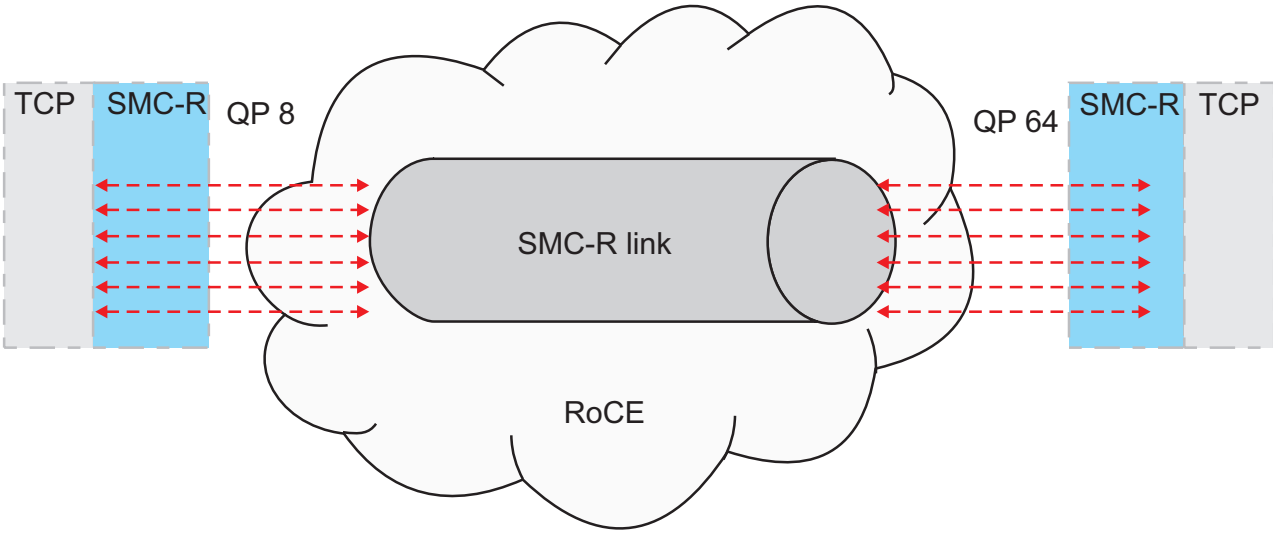


Figure 7. Multiple TCP connections over one SMC-R link

SMC-R link groups: A Shared Memory Communications over RDMA (SMC-R) link group is a logical grouping of SMC-R links between two communicating peers, as shown in Figure 8 on page 21. An SMC-R link group is formed when the initial SMC-R link is established between two peers.

All SMC-R links in an SMC-R link group must be *equal* links. SMC-R links are considered to be equal when all of the following conditions are true:

- The links provide access to the same RDMA memory buffers at the remote peer virtual servers.
- The links have the same VLAN ID, or they do not use a VLAN ID.
- The links have the same TCP server and TCP client roles or relationship.

  A peer that is acting as the TCP connection server has different responsibilities for establishing and maintaining SMC-R communications than a peer that is acting as the TCP connection client. Unique SMC-R link groups are established between two peers when the peers act as both servers and clients for TCP connections.

When the initial SMC-R link is established and a second IBM 10GbE RoCE Express interface is available, Communications Server establishes an equal SMC-R link between the peers. The 10GbE RoCE Express interfaces are shown as RNICs in Figure 8 on page 21.

Adding a second SMC-R link to the SMC-R link group provides the following benefits:

- High availability

  To maintain high availability, you need two SMC-R links between SMC-R peers. If a failure occurs with one SMC-R link, TCP connections that are using the failing SMC-R link are switched to the other active link in the link group and disruptions to application workloads are avoided. For more information, see "SMC-R high availability considerations" on page 29.
- Workload balancing

  TCP connections are distributed across the SMC-R links in a link group, increasing bandwidth and avoiding bottlenecks.

Rule: Workload balancing within an SMC-R link group occurs only when both the local and the remote peers have two 10GbE RoCE Express interfaces, and thus two SMC-R links are established in the link group.

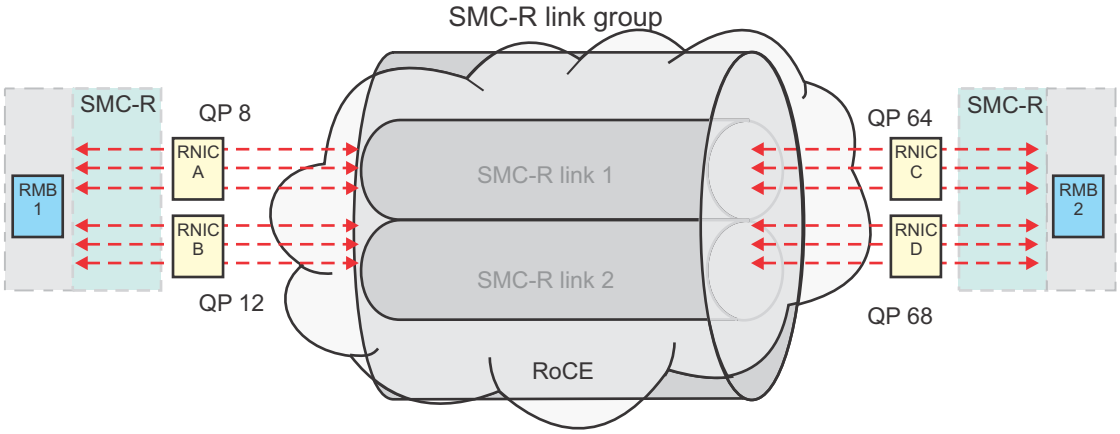


Figure 8. SMC-R link group

Because SMC-R links within a link group are considered equal, TCP connections can be assigned to any SMC-R link within the group. Furthermore, the client and the server can choose to assign the TCP connection to different SMC-R links within the group, and can move the TCP connections from one SMC-R link to another within the group. For example, in Figure 8, client traffic might flow over one SMC-R link (between RNICs A and C) and server traffic might flow over the other SMC-R link (between RNICs B and D). The peers do not have to exchange knowledge of which physical 10GbE RoCE Express interface is being used for data transmission, and the recipient is only aware that data was placed into the RDMA memory buffer.

An SMC-R link group remains active for up to 10 minutes after the last TCP connection that is using the link group is stopped.

SMC-D links: After two Shared Memory Communications - Direct Memory Access (SMC-D) peers recognize during rendezvous processing that shared memory communications are possible, a logical SMC-D link is established between the peers by using internal shared memory (ISM). An SMC-D link, as shown in Figure 9 on page 22, is uniquely defined by a combination of the following information:

- Remote and local global ID (GID) values

  An SMC-D GID is an 8-byte value that the ISM device assigns.
- Virtual LAN (VLAN) ID

  You can optionally use VLANs to isolate application traffic into different virtual networks on the same physical Ethernet or HiperSockets CHPID.
  - If you use VLANs, the VLAN ID that is specified on the IPAQENET, IPAQENET6, IPAQIDIO, or IPAQIDIO6 INTERFACE statement is used as an attribute to create unique SMC-D links between the peers for unique VLANs. In other words, the SMC-D links are VLAN qualified.
  - If you do not use VLANs, no VLAN ID is used to define the SMC-D links between the peers. In other words, the SMC-D links are not VLAN qualified.

  For more information about using VLANs, see “VLANID considerations” on page 25.

If the application traffic that is between the two peers uses the same remote and local GIDs, and is associated with the same VLAN when VLANs are defined, the application traffic can use the same SMC-D link.

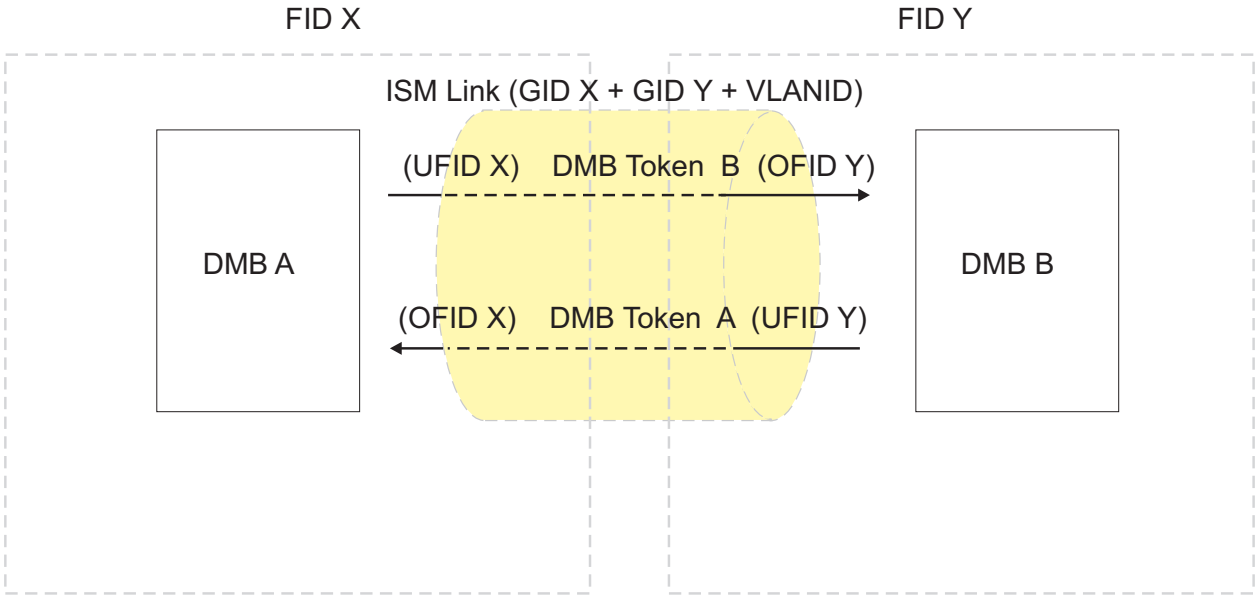


Figure 9. Identifying an SMC-D link

Besides the 3-tuple (local GID + remote GID + VLAN ID) that uniquely defines an SMC-D link, each peer assigns a 4-byte SMC-D link ID that uniquely identifies the SMC-D link within its own resource space. This SMC-D link ID is exchanged between peers and can be used for network management and diagnostic purposes. For instance, you can use the SMC-D link ID to filter Netstat report information that is related to a specific SMC-D link. For more information, see "Displaying SMC information" on page 48.

An SMC-D link supports multiple TCP connections between the same two peers. The first TCP connection between the peers establishes the SMC-D link, and subsequent TCP connections between the peers can use the previously established link.

SMC memory buffers

Each stack locally allocates memory for an SMC memory buffer to receive inbound data that uses SMC communications. An SMC memory buffer that is used for SMC-R communications is called a remote memory buffer (RMB), and an SMC memory buffer that is used for SMC-D communications is called a direct memory buffer (DMB). The sending operating system places TCP socket application data directly into the memory buffer that the receiving stack assigns to receive data for a TCP connection. The receiving stack then copies the data from the memory buffer into the receive buffer of the receiving socket application.

A memory buffer is partitioned into elements of equal size, and each element is associated with a single TCP connection. Direct memory buffers are partitioned into direct memory buffer elements (DMBEs), and remote memory buffers are partitioned into remote memory buffer elements (RMBEs). In the Connection Layer Control (CLC) messages during rendezvous processing, each peer communicates the location of its local DMBE, or its RMBE and a remote key, to allow remote

access to the memory buffer. The remote host has write access and the local host reads the data for passing to the socket application.

SMC-R usage of memory buffers: For z/OS Communications Server, an RMB is a contiguous, 1-MB block of fixed 64-bit private storage. In Figure 10, an RMB is created on z/OS, into which the peer node can write, and an RMB is created on the peer node, into which z/OS can write. An RMB must be registered with the IBM 10GbE RoCE Express interface so that the storage is available to the remote peer.

Each RMB is associated with the reliable connected queue pairs (RC QPs) and therefore with the SMC-R link for the two communicating peers. The association of the RMB to the RC QPs ensures that only the two peers have RDMA access to this particular RMB. In addition, all RMBs that are associated with a particular SMC-R link must be accessible to the remote peer by using any SMC-R link in the link group. This accessibility enables the remote peer to use any link within the link group to place the TCP connection data into the correct RMB.

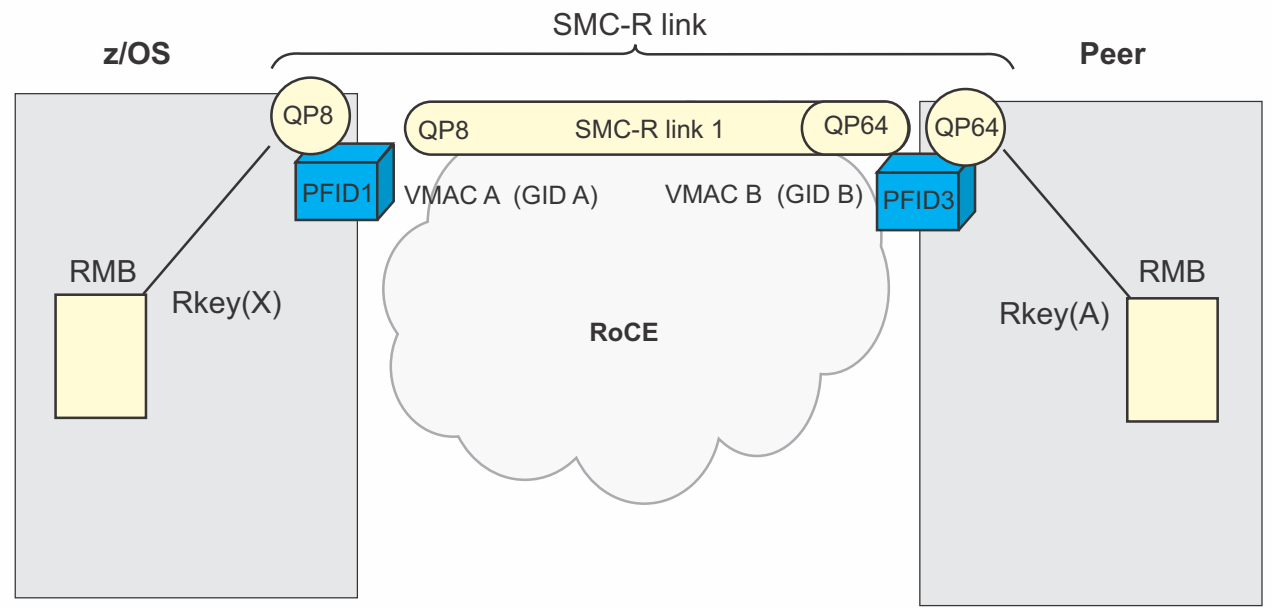


Figure 10. RMBs assigned to an SMC-R link

The SMC-R peers are not required to assign RMBEs of the same size for the client and the server of a specific TCP connection. The peers can use one or more RMBs for the TCP connections that are using the same SMC-R link.

When an SMC-R link group is first established, z/OS Communications Server allocates a basic set of three RMBs for the link group. The RMBE sizes for the RMBs are not defined initially, but instead are determined by the needs of the TCP connections that use the SMC-R link. z/OS Communications Server uses RMBE sizes of 32 KB, 64 KB, 128 KB, 256 KB, and greater than 256 KB. The appropriate size for the TCP connection is selected based on the receive buffer size of the local application. When the application does not explicitly set the buffer size by using SETSOCKOPT(), the default value is determined by the value of the TCPRCVBUFRSIZE parameter on the TCPCONFIG statement.

More RMBs are allocated as needed to accommodate more TCP connections or different receive buffer sizes.

SMC-D usage of memory buffers: For z/OS Communications Server, a DMB is a contiguous, 1 MB block of pinned 64-bit private storage. A DMB is created on z/OS, into which the peer node can write, and a DMB is created on the peer node, into which z/OS can write. A DMB must be registered with the ISM interface so that the storage is available to the remote peer. Each DMB is associated with one and only one SMC-D link.

The SMC-D peers are not required to assign DMBEs of the same size for the client and the server of a specific TCP connection. The peers can use one or more DMBs for the TCP connections that are using the same SMC-D link.

When an SMC-D link is first established, z/OS Communications Server allocates a basic set of three DMBs for the link. The DMBE sizes for the DMBs are not defined initially, but instead are determined by the needs of the TCP connections that use the SMC-D link. z/OS Communications Server uses DMBE sizes of 64 KB, 128 KB, 256 KB, and greater than 256 KB. The appropriate size for the TCP connection is selected based on the receive buffer size of the local application. When the application does not explicitly set the buffer size by using SETSOCKOPT(), the default value is determined by the value of the TCPRCVBUFRSIZE parameter on the TCPCONFIG statement.

More DMBs are allocated as needed to accommodate more TCP connections or different receive buffer sizes.

SMC-R staging buffers

Each TCP/IP stack allocates 64-bit fixed private staging buffer memory for outbound Shared Memory Communications over RDMA (SMC-R) data. Staging buffers are not associated with specific SMC-R links or link groups, but are used by all TCP connections that traverse SMC-R links on this stack.

Like remote memory buffers (RMBs), staging buffers are 1 MB in length and must be registered with the IBM 10GbE RoCE Express interface before they are used for SMC-R communications. Unlike RMBs, the address of the staging buffer is not shared with the remote SMC-R peer because only local applications access the staging buffer storage.

z/OS Communications Server allocates 4 MB of staging buffer storage when the first 10GbE RoCE Express interface is activated, and allocates more buffers as necessary to accommodate application workloads.

Using Shared Memory Communications

There are some configuration considerations and environment setup steps before you can configure and use Shared Memory Communications over RDMA (SMC-R) or Shared Memory Communications - Direct Memory Access (SMC-D).

Tip: You can use the SMC Applicability Tool (SMCAT) report to better understand the amount of your TCP workload that can use SMC communications. For more information about the SMCAT, see z/OS Communications Server: IP System Administrator's Commands.

Configuration considerations for Shared Memory Communications

Before you configure Shared Memory Communications, consider the following factors:

- Decide whether to use VLANs. For more information, see "VLANID considerations."
- Identify the physical connections between stacks and SMC devices. For more information, see "Physical network considerations" on page 26.
- Provide physical redundancy for high availability when using SMC-R. For more information, see "SMC-R high availability considerations" on page 29.
- Verify the system and network requirements.
  - For more information about system requirements for SMC-R, see "System requirements for SMC-R in a dedicated RoCE environment" on page 34, "System requirements for SMC-R in a shared RoCE environment" on page 35, and "Network requirements for SMC-R" on page 36.
  - For more information about system requirements for SMC-D, see "System requirements for SMC-D" on page 36.

VLANID considerations:

The VLANID operand is optional on the following SMC capable interfaces:

- IPAQENET and IPAQENET6 INTERFACE statements with the OSD channel path ID type (CHPIDTYPE OSD)
- IPAQIDIO and IPAQIDIO6 INTERFACE statements (SMC-D support only)

On a specific OSA or HiperSockets transport resource list element (TRLE) basis, z/OS Communications Server enforces consistent VLAN definitions for INTERFACE statements that are associated with the same OSA or HiperSockets TRLE.

For example, when VLANs are not used, the stack configuration allows only a single INTERFACE statement, and the VLANID operand is omitted on that INTERFACE statement. When VLANs are used, multiple INTERFACE statements are allowed and each INTERFACE statement must specify a unique VLANID value.

The OSD VLAN attributes of the IPAQENET or IPAQENET6 interface are propagated to the IBM 10GbE RoCE Express interfaces (associated RNIC) or ISM interfaces (associated ISM) that have the same physical network identifier (PNetID) value. The HiperSockets VLAN attributes on the IPAQIDIO or IPAQIDIO6 interface are propagated to the ISM interfaces that have the same PNetID value. See Physical network considerations for more details on PNetID.

SMC-R VLANID usage

Whether SMC-R communications use virtual LANs depends on the definition of the SMC-R capable OSD interfaces that are extended to the associated 10GbE RoCE Express interfaces. The 10GbE RoCE Express feature can be shared by TCP/IP stacks that are configured to use different VLAN capabilities for the 10GbE RoCE Express feature. You can use up to 126 unique VLANID values per RoCE Express port.

Depending on the operating mode, the number of VLANID values that can be used per 10GbE RoCE Express feature has the following limits:

- When the RoCE Express feature operates in a dedicated RoCE environment, up to 126 unique VLANID values can be used per port.
- When the RoCE Express feature operates in a shared RoCE environment, up to 126 unique VLANID values can be used per port. In addition, each virtual function (VF) PFID representation of the feature can use up to 16 VLANID

values, although internal RoCE Express feature limitations might further reduce that maximum value for individual PFID representations.

Result: Multiple VF representations of the same RoCE Express feature can use the same VLANID value, and only one of the available 126 VLANID values is used.

Result: If you define more unique VLANID values for one PNetID on the SMC-R capable INTERFACE statements than the 10GbE RoCE Express feature can support, the VLANID values of the last INTERFACE statements to be activated are not registered with the 10GbE RoCE Express feature. The IPAQENET or IPAQENET6 interfaces can start, but TCP connections that are established over these interfaces cannot use SMC-R communications. Netstat ALL/-A reports that display the TCP connections include the following diagnostic information for the connection:

```
SMCRSTATUS:        INACTIVE
SMCREASON:        00005206 - VLAN ID NOT FOUND
```

SMC-D VLANID usage

Whether SMC-D communications use virtual LANs depends on the definition of the SMC-D capable OSD or HiperSockets interfaces that are extended to the associated ISM interfaces. The ISM device can be shared by TCP/IP stacks that are configured to use different VLAN capabilities for the ISM device. Each TCP/IP stack, or virtual function (VF), can use up to 64 unique VLANID values per ISM interface.

Result: If you define more unique VLANID values for one PNetID on the SMC-D capable INTERFACE statements than the ISM device can support, the VLANID values of the last INTERFACE statements to be activated are not registered with the ISM device. The IPAQENET, IPAQENET6, IPAQIDIO, or IPAQIDIO6 interfaces can start, but TCP connections that are established over these interfaces cannot use SMC-D communications. Netstat ALL/-A reports that display the TCP connections include the following diagnostic information for the connection:

```
SMCDSTATUS:        INACTIVE
SMCREASON:        00005206 - VLAN ID NOT FOUND
```

Physical network considerations:
The TCP/IP stack must be able to determine which physical network is connected to a particular 10GbE RoCE Express or ISM interface, so that the interface can be associated with the SMC capable IPAQENET, IPAQENET6, IPAQIDIO, and IPAQIDIO6 interfaces that connect to that same physical network. For example, in Figure 11 on page 27, three distinct and physically separated networks can be accessed by using SMC-R communications.

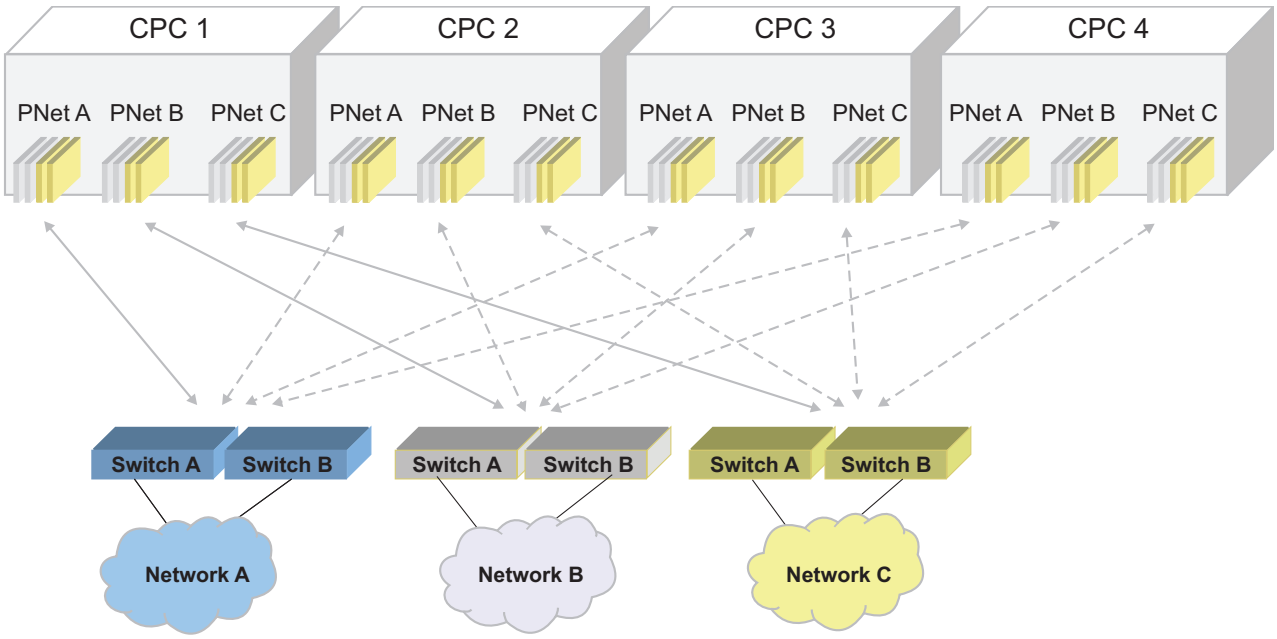


Figure 11. Physical networks

The concept of a physical network identifier (PNetID) was created to simplify this physical network configuration task. With the convention of a PNetID, you can define a value to represent the ID or name of your physical layer 2 LAN fabric or physical broadcast domain. The System z physical ports that are to be connected to the associated physical networks are then logically associated with their respective PNetIDs. The PNetID then becomes an attribute of the physical port of the feature or adapter, describing how this feature or adapter is physically connected to your data center network. You can specify the PNetID in a single step within the hardware configuration definition (HCD), enabling all operating systems of all associated CPCs to dynamically learn and use this definition.

You can use virtual LANs (VLANs) to logically separate a physical network. If you configure multiple PNetIDs for SMC-R or SMC-D, then you must ensure that each VLAN or subnet in your configuration does not span more than one PNetID. The physical network that a PNetID represents can include multiple subnets, but each subnet must correspond to a specific PNetID.

SMC processing requires the use of subnet masks. For more information, see "Configuring Shared Memory Communications over RDMA" on page 37 and "Configuring Shared Memory Communications - Direct Memory Access" on page 40.

For more information about the HCD, see z/OS HCD Planning and z/OS HCD User's Guide.

SMC-R physical network considerations

A physically separate IBM 10GbE RoCE Express feature is provided to use RDMA over Converged Ethernet (RoCE) on System z. This feature is used with the existing Ethernet connectivity that OSA provides. The 10GbE RoCE Express feature provides access to the same physical Ethernet fabric that is used for traditional IP connectivity. For more information about the Ethernet switch requirements for

RoCE, see "Setting up the environment for Shared Memory Communications over RDMA" on page 37 and *IBM z Systems™ Planning for Fiber Optic Links*.

The operating systems must logically group the associated physical ports of both the 10GbE RoCE Express and OSA adapters based on their required physical connectivity. Each central processor complex (CPC) connects to a physical network by using both OSA and 10GbE RoCE Express ports. You can use two RoCE Express ports at most to connect to a physical network at a given time, but you can use as many OSA adapters as necessary for your network bandwidth or usage requirements. An example of this logical grouping, using two OSA adapters and two RoCE Express features, is shown in Figure 11 on page 27.

One TCP/IP stack can define up to 16 Peripheral Component Interconnect Express (PCIe) function ID (PFID) values. Each PFID value must match a FID value configured in the hardware configuration definition (HCD).

- In a dedicated RoCE environment, each PFID represents a unique PCHID definition of a RoCE Express feature, and only one of the two RoCE Express ports for the feature can be used at a time.
- In a shared RoCE environment, each PFID represents a virtual function (VF) usage of a RoCE Express feature, and multiple PFID values can be associated with the same physical feature and port.

To match the 10GbE RoCE Express features with the correct OSA SMC-R capable adapters, you must define a PNetID value for both the 10GbE RoCE Express interface (physical port) and the corresponding OSA adapters (physical port) within the HCD. The OSA ports correspond to the stack IPAQENET and IPAQENET6 interfaces. VTAM and the TCP/IP stack then dynamically learn the PNet IDs for the 10GbE RoCE Express interface and the OSA interfaces when the 10GbE RoCE Express interface or the OSD interface is started. The 10GbE RoCE Express interface is associated with only SMC-R capable OSA interfaces that have the same PNetID value defined.

Guideline: The TCP/IP stack does not validate the layer 2 physical network topology or broadcast domain. PNet IDs are values that you assign, and the operating systems learn and use these assigned values but cannot validate them within the Ethernet switched fabric. Therefore, the operating system does not assure or enforce any physical network separation or isolation across different physical networks. To physically isolate unique physical networks, you must ensure that traffic on network A cannot reach hosts on network B.

SMC-D Physical Network considerations

The ISM device does not connect to the same Ethernet fabric that the SMC-D capable OSA interfaces use. However, the operating systems must still logically group the ISM device with the OSA or HiperSockets interfaces based on their required physical connectivity. When z/OS Communications Server activates the first SMC-D capable interface for a given physical network, it also attempts to activate an ISM interface for that same physical network. The Peripheral Component Interconnect Express (PCIe) function ID (PFID) value that represents the ISM device is obtained during activation processing. The possible PFID values to use for ISM devices are configured in the hardware configuration definition (HCD).

To match the ISM device with the correct SMC-D capable OSA or HiperSockets adapters, you must define a PNetID value for both the ISM device and the

corresponding OSA or HiperSockets adapter within the HCD. The OSA ports correspond to the stack IPAQENET and IPAQENET6 interfaces, and the HiperSockets adapters correspond to the stack IPAQIDIO and IPAQIDIO6 interfaces. VTAM and the TCP/IP stack dynamically obtain the PNetIDs for the ISM, OSA, and HiperSockets interfaces when the interface is started. The ISM interface is associated with only SMC-D capable OSA or HiperSockets interfaces that have the same PNetID value defined.

Guideline: The same physical network cannot be used for OSA and HiperSockets interfaces.

SMC-R high availability considerations: Shared Memory Communications over RDMA (SMC-R) enables high-speed peer-to-peer connections over the RDMA over Converged Ethernet (RoCE) fabric between reliable connected queue pairs (RC QPs). SMC-R defines the RC QPs as an SMC-R link, and SMC-R links are logically grouped into SMC-R link groups. For more information, see "SMC-R links" on page 18 and "SMC-R link groups" on page 20.

IBM 10GbE RoCE Express features at each host are required for SMC-R communications. After a TCP connection dynamically and successfully switches to SMC-R, it cannot revert to standard TCP/IP communications. Therefore, to achieve network high availability for SMC-R, it is critical to provide redundant physical network connectivity.

If the underlying 10GbE RoCE Express interface or the associated network hardware fails, the z/OS host provides dynamic failover processing that transparently moves the TCP connections from the SMC-R links that are using the failed 10GbE RoCE Express interface to another SMC-R link in the link group. If no other SMC-R link in the link group is available at the time of failure, the TCP connections are lost. To have a second redundant SMC-R link within a link group, two 10GbE RoCE Express interfaces must be defined and active.

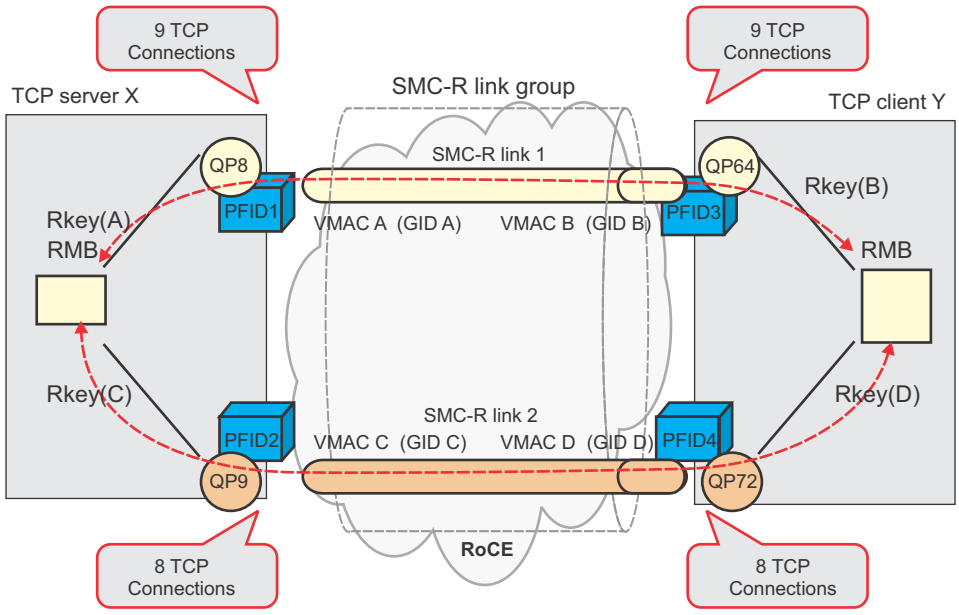


Figure 12. Redundant SMC-R links in an SMC-R link group

If the 10GbE RoCE Express interfaces operate in a shared RoCE environment , an SMC-R link group might be considered redundant, even though the 10GbE RoCE Express interfaces associated with SMC-R links use the same physical 10GbE RoCE Express feature.

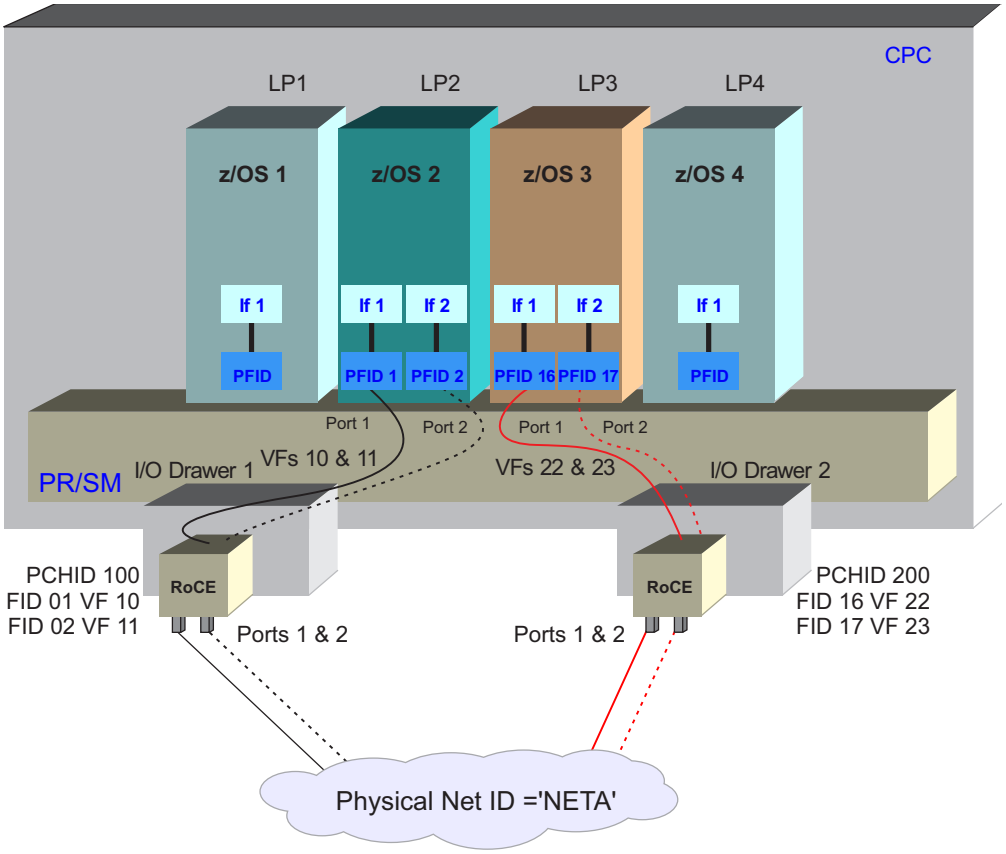


Figure 13. Misleading full redundancy configuration in a shared RoCE environment

For instance, in Figure 13, z/OS 2 has multiple PFID values defined, but the PFID values represent different ports on the same 10GbE RoCE Express feature. When TCP connections that use SMC-R are established in this configuration, an SMC-R link group, with two SMC-R links, is created. The two SMC-R links make this SMC-R link group appear to have full redundancy, but an failure involving the 10GbE RoCE Express feature will result in failures of both PFIDs and all the associated interfaces. This in turn will cause failures for both SMC-R links within the SMC-R link group. As a result, dynamic failover processing will not occur, and TCP connections that use those SMC-R links will fail. A configuration of this type is identified by a value of "Partial (single local PCHID, unique ports)" in Netstat Devlinks/-d reports involving the SMC-R link group. For more information, see Redundancy levels.

To ensure that a redundant path exists in a shared RoCE environment, you must design your connectivity to ensure that the PFID values used by a given TCP/IP stack represent physically different 10GbE RoCE Express features. Two 10GbE RoCE Express features are physically different if they are configured with different PCHID values. See Figure 3 on page 11 for an example of using physically different 10GbE RoCE Express features in a shared RoCE environment.

As shown in Figure 12 on page 29, when both SMC-R peers have two active 10GbE RoCE Express interfaces, TCP connections are distributed across the links. TCP connection data can use either SMC-R link, even if the TCP connection is considered to be assigned to a specific SMC-R link.

If a failure is experienced involving one SMC-R link, all the TCP connections are moved automatically to the other SMC-R link. For example, as shown in Figure 14, when SMC-R link 2 fails, all connections are moved to SMC-R link 1. After recovery, when a new SMC-R link is established, new TCP/IP connections are moved to the new link to balance utilization of the RoCE physical resources. Existing connection might also be moved to the new link.

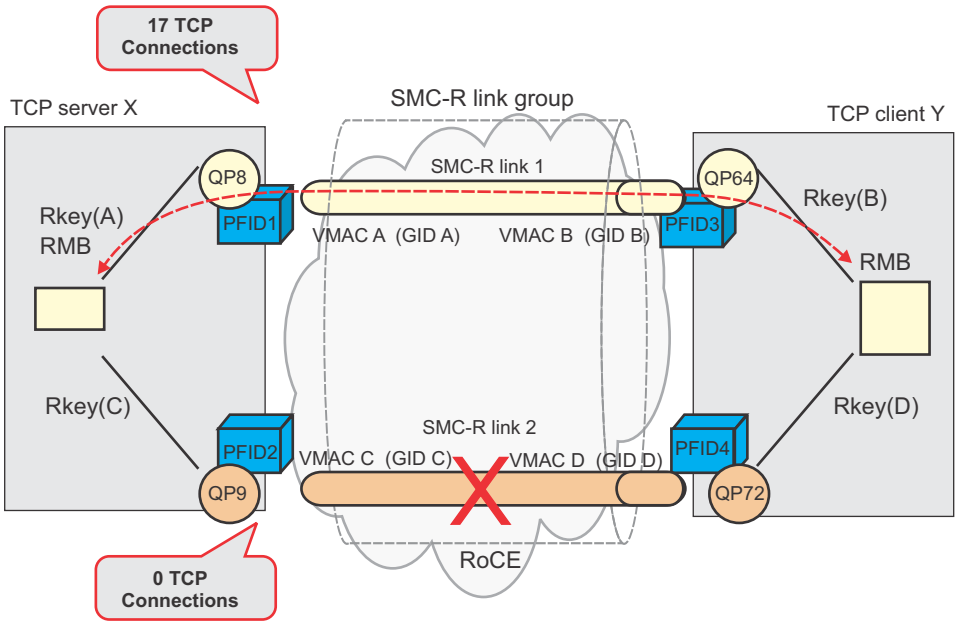


Figure 14. Failover processing within an SMC-R link group

Figure 12 on page 29 and Figure 14 do not show the RoCE switches, but ideally, redundant physical switches are also present.

If both SMC-R peers do not have multiple active 10GbE RoCE Express interfaces, then the SMC-R link group does not provide an ideal level of TCP connection resiliency. Figure 15 on page 32 is an example of a configuration where one peer (the server host) has two active 10GbE RoCE Express interfaces, but the other peer (the client host) has just one. In this situation, the server still creates two SMC-R links, one per active interface, so the server can still move the TCP connections between SMC-R links if a 10GbE RoCE Express interface fails. The client, however, cannot move the TCP connections if its 10GbE RoCE Express interface fails because no alternative path exists. Because only one peer can provide recovery capability, this configuration has partial redundancy.

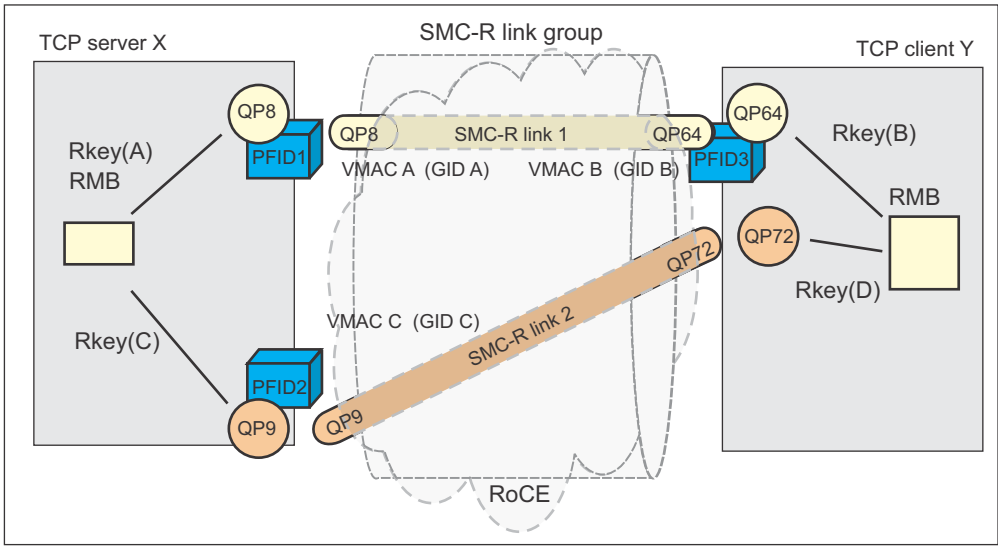


Figure 15. Partially redundant SMC-R links

If neither the server or the client has multiple active 10GbE RoCE Express interfaces, as shown in Figure 16, then the SMC-R link group is composed of a single SMC-R link. If a 10GbE RoCE Express interface fails in this configuration, the TCP connections cannot be recovered or moved, so they are all lost. This type of SMC-R link is called a single link, and the configuration has no redundancy capability.

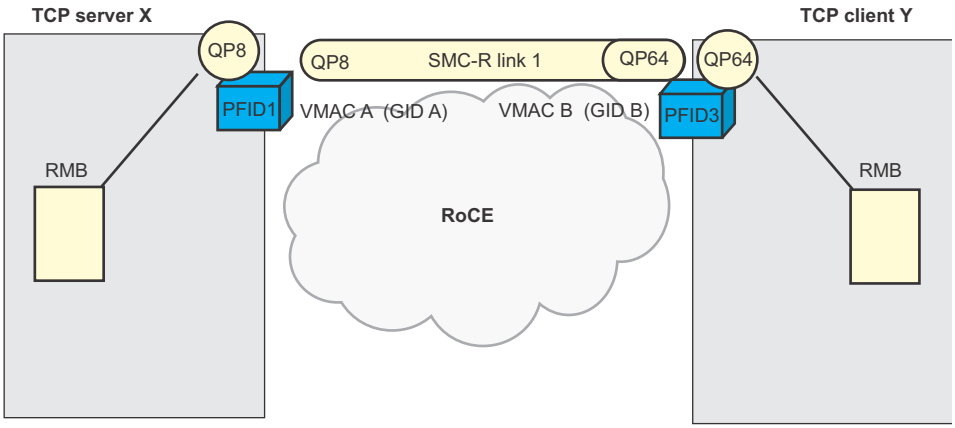


Figure 16. SMC-R link group with no redundant link

Redundancy levels

System z also provides redundant internal Peripheral Component Interconnect Express (PCIe) hardware support infrastructures for the PCIe-based 10GbE RoCE Express features. For simplicity, the System z internal PCIe infrastructure is referred to as the *internal path*. The internal path of the 10GbE RoCE Express feature is determined based on how the feature is plugged into the System z I/O drawers. To have full 10GbE RoCE Express hardware redundancy on System z, each feature must have unique internal paths. For more information about the System z I/O drawer configurations, see your IBM Service representative.

A complete high availability solution, therefore, requires the following setup between two SMC-R peers:

- Two unique physical 10GbE RoCE Express features that use unique PCHIDs (see "SMC-R high availability considerations" on page 29)
- Unique system PCIe support infrastructures, or internal paths, for the two features
- Unique physical RoCE switches

From the perspective of the local stack, the physical network topology and the internal path configuration at the remote system to the remote adapters are not visible. z/OS Communications Server can evaluate and report a redundancy level that is based only on the known local factors. If the local stack has two unique 10GbE RoCE Express features that have unique internal paths, then an SMC-R link group with two redundant SMC-R links is considered to have full redundancy.

Table 3 shows the reported redundancy levels with a description of each level. The values that are listed here represent the values that are displayed for an SMC-R link group in a Netstat DEVlinks/-d report. For an example of the Netstat DEvlinks/-d report, see z/OS Communications Server: IP System Administrator's Commands.

Table 3. Redundancy levels

Redundancy level	SMC-R link group with redundant links	Unique 10GbE RoCE Express features have unique physical internal paths	Description
Full	Yes	Yes	Full local hardware redundancy **Rule:** Hardware redundancy must be verified at each host. The internal path at the remote host is not visible to the local host and therefore is not considered.
Partial (single local internal path)	Yes	No	The local 10GbE RoCE Express features share an internal System z PCIe adapter support infrastructure (hardware internal path). This hardware configuration provides a single point of failure, so full redundancy cannot be guaranteed.
Partial (single local PCHID, unique ports)	Yes	No	The local 10GbE RoCE Express features use the same PCHID but unique ports. Using the same PCHID creates a single point of failure, so full redundancy cannot be guaranteed.
Partial (single local PCHID and port)	Yes	No	The local 10GbE RoCE Express features use the same PCHID and port. Using the same PCHID and port creates a single point of failure, so full redundancy cannot be guaranteed.
Partial (single local RNIC)	No	N/A	The link group has only a single active feature on the local host, but multiple active features are available to the remote host.
Partial (single remote RNIC)	No	N/A	The link group has only a single active feature on the remote host, but multiple active features on the local host.
None (single local and remote RNIC)	No	N/A	The link group has only a single active feature on both the local and the remote host.

A 10GbE RoCE Express interface that is associated with an SMC-R capable interface because it has the same physical network ID is referred to as an *associated RNIC interface*. More than two 10GbE RoCE Express interfaces can be defined with the same physical network ID, but the TCP/IP stack creates SMC-R link groups

that use no more than two associated RNIC interfaces at any particular time. The 10GbE RoCE Express interfaces are considered to be associated RNIC interfaces for IPAQENET and IPAQENET6 interfaces that match all of the following characteristics:

- The interfaces are active.
- The interfaces are defined by the INTERFACE statement with the OSD channel path ID type (CHPIDTYPE OSD).
- The interfaces are enabled for SMC-R communications.
- The interfaces have matching PNetID values.

Associated RNIC interfaces are displayed in the Netstat DEvlinks/-d OSD report. For an example of the Netstat DEvlinks/-d report, see z/OS Communications Server: IP System Administrator's Commands.

Any additional 10GbE RoCE Express interfaces that have the matching PNetID are started, but they are not used to provide for added link level load-balancing purposes. Instead, the extra 10GbE RoCE Express interfaces are held in reserve for use if one of the associated RNIC interfaces fails.

For instance, in Figure 14 on page 31, if 10GbE RoCE Express interface 2 (shown as PFID2) on the server host fails, the TCP connections that were using SMC-R link 2 across interface 2 are switched to SMC-R link 1. The SMC-R link group loses its level of full link redundancy because only SMC-R link 1 is active. However, if another 10GbE RoCE Express interface, call it PFID 5, were active on the server host, and PFID 5 had the same PNetID value as PFID 1 and PFID 2, the server can immediately activate new SMC-R links across PFID 5 to the client host to reestablish full link redundancy. If PFID 5 and PFID 1 have unique physical paths, then full redundancy is also restored. This new SMC-R link is used for TCP connections within the link group. If PFID 2 recovers, it now serves as a standby PFID and can be used if either PFID 1 or PFID 5 fails.

You can also use extra PFIDs for planned outages, such as to schedule an upgrade to the 10GbE RoCE Express features.

System and network requirements for Shared Memory Communications:
Depending on what type of Shared Memory Communications (SMC) you will use, the system requirements are different. In addition, SMC-R imposes additional network requirements.

If you will use both SMC-R and SMC-D, you must ensure that the system and network requirements for each type of processing are met.

System requirements for SMC-R in a dedicated RoCE environment:

You need to ensure that your system meets the requirements to use SMC-R with RoCE Express features operating in a dedicated RoCE environment.

A z/OS image must be z/OS Version 2 Release 1 or later to use Shared Memory Communications over RDMA (SMC-R) with RoCE Express features operating in a dedicated RoCE environment.

SMC-R requires RDMA over Converged Ethernet (RoCE) hardware and firmware support. The following minimum hardware requirements must be met to use SMC-R:

- You must have an IBM zEnterprise EC12 (zEC12) with driver 15, or an IBM zEnterprise BC12 (zBC12).
- You must have one or more IBM 10GbE RoCE Express features.

  10GbE RoCE Express features are dual ports with short range (SR) optics and dedicated to a single LPAR image.

  Guideline: Provide two 10GbE RoCE Express features per z/OS image per unique physical network. For more information, see "RoCE network high availability" on page 36.
- You must have System z OSA-Express for traditional Ethernet LAN connectivity using CHPID type OSD.

  SMC-R does not impose any specific OSA requirements.
- You must have standard 10 GbE switches.

System requirements for SMC-R in a shared RoCE environment:

You need to ensure that your system meets the requirements to use SMC-R with RoCE Express features operating in a shared RoCE environment.

To use Shared Memory Communications over RDMA (SMC-R) with RoCE Express features operating in a shared RoCE environment, the minimum software requirement must be z/OS Version 2 Release 1 with APARs OA44576 and PI12223 applied.

SMC-R requires RDMA over Converged Ethernet (RoCE) hardware and firmware support. The following minimum hardware requirements must be met to use SMC-R:

- You must have IBM z13 (z13) or later systems.
- You must have one or more IBM 10GbE RoCE Express features.

  10GbE RoCE Express features are dual ports with short range (SR) optics and can be shared across multiple operating systems images or TCP/IP stacks in a central processor complex (CPC).

  Guideline: Provide two 10GbE RoCE Express features per unique physical network. For more information, see "RoCE network high availability" on page 36.
- You must have System z OSA-Express for traditional Ethernet LAN connectivity.

  SMC-R does not impose any specific OSA requirements.
- You must have standard 10 GbE switches.
- If you configure more than 24 Peripheral Component Interconnect Express (PCIe) devices, you must configure the IEASYSxx LFAREA parameter. The 24 PCIe devices include all z/OS Communications Server PCIe devices and other z/OS PCIe devices. In z/OS Communications Server, you can configure the following PCIe devices:
  - IBM 10GbE RoCE Express features
  - Internal shared memory (ISM) devices

  For more information about specifying the IEASYSxx LFAREA parameter, see z/OS MVS Initialization and Tuning Guide.

Network requirements for SMC-R:

You need to ensure that your system meets the network requirements to use SMC-R with RoCE Express features.

z/OS Communications Server supports connectivity to multiple, distinct layer 2 networks through unique physical LANs. Each unique physical network is identified by existing Ethernet standards that are based on the physical layer 2 broadcast domain. You can define a physical network ID (PNetID) for each physical network. For more information, see "SMC-R physical network considerations" on page 27.

For hosts to communicate by using SMC-R, they must connect directly to the same Ethernet layer 2 LAN network. If VLANs are in use, each host must also have access to the same VLAN. For more information, see "SMC-R VLANID usage" on page 25.

There are restrictions on the physical distances that can be used to route RDMA frames. To understand these distance specifications and limitations, see *IBM z Systems Planning for Fiber Optic Links*.

RoCE network high availability

Because RoCE connections do not use IP routing and the RDMA connections to remote hosts are direct point-to-point connections that use reliable connected queue pairs (RC QPs), there is no concept of an alternative IP route to the peer. SMC-R connectivity is possible with a single 10GbE RoCE Express feature, but a loss in that single feature means that the associated TCP connections and workloads are disrupted. Therefore, redundant 10GbE RoCE Express features on both the local and remote hosts are required to achieve network high availability with SMC-R. If your TCP workloads require high availability, redundant 10GbE RoCE Express features and redundant Ethernet switches are required. The SMC-R protocol actively uses both features, rather than using one feature with the other in standby mode. For more information, see "SMC-R high availability considerations" on page 29.

IBM 10GbE RoCE Express features also have redundant internal PCIe support structures, or PCIe internal paths, as described in "Redundancy levels" on page 32. To avoid another single point of failure, install each 10GbE RoCE Express feature that is managed by the same operating system with a unique internal path. For more information about how to install a 10GbE RoCE Express feature to achieve full redundancy, see your IBM service representative.

RoCE bandwidth

The 10GbE RoCE Express features provide 10 GbE ports. When redundant features are defined, SMC-R link groups can be formed by using both features, resulting in a 20 GbE logical pipe to each physical network. z/OS Communications Server uses only two features within a link group at any particular time.

System requirements for SMC-D:

You need to ensure that your system meets the system requirements to use SMC-D.

To use Shared Memory Communications - Direct Memory Access (SMC-D), the minimum software requirement is z/OS Version 2 Release 2 with APARs OA48411 and PI45028 applied, and the minimum hardware requirement is IBM z13 GA2 or later systems.

If you configure more than 24 Peripheral Component Interconnect Express (PCIe) devices, you must configure the IEASYSxx LFAREA parameter. The 24 PCIe devices include all z/OS Communications Server PCIe devices and other z/OS PCIe devices. In z/OS Communications Server, you can configure the following PCIe devices:

- IBM 10GbE RoCE Express features
- Internal shared memory (ISM) devices

For more information about specifying the IEASYSxx LFAREA parameter, see z/OS MVS Initialization and Tuning Guide.

Setting up the environment for Shared Memory Communications over RDMA

Before you configure Shared Memory Communications over RDMA (SMC-R), follow these steps to ensure that other components are configured.

Before you begin

Review "Configuration considerations for Shared Memory Communications" on page 24.

Procedure

Perform the following steps to prepare to use SMC-R:

1. Install and configure the IBM 10GbE RoCE Express features in the hardware configuration definition (HCD). Logical partition (LPAR) access lists must be provided for the 10GbE RoCE Express features.
2. Assign physical network ID (PNetID) values, and configure the values in the HCD for both the 10GbE RoCE Express ports and any OSA-Express devices that will use the 10GbE RoCE Express ports for SMC-R communications.
3. Provide for redundant system PCIe internal paths for the defined IBM 10GbE RoCE Express features. For more information, see "Redundancy levels" on page 32.
4. Configure Ethernet switches for RDMA functionality. RDMA processing requires standard 10 GbE switch support, and distance limitations might exist. Enable the global pause frame (a standard Ethernet switch feature for Ethernet flow control that is described in the IEEE 802.3x standard) on the switch. You might also need to configure the switch to indicate whether you use VLANs.

   For more information, see "Network requirements for SMC-R" on page 36.

Configuring Shared Memory Communications over RDMA

Use these steps to configure and begin to use Shared Memory Communications over RDMA (SMC-R).

Before you begin

See "Setting up the environment for Shared Memory Communications over RDMA."

Procedure

Perform the following steps to configure SMC-R:

1. If necessary, convert IPv4 IPAQENET DEVICE, LINK, and HOME definitions to INTERFACE definitions. SMC-R processing is provided only for OSD interfaces configured with INTERFACE definitions. For more information about converting IPv4 IPAQENET DEVICE, LINK, and HOME definitions to INTERFACE definitions, see Steps for converting from IPv4 IPAQENET DEVICE, LINK, and HOME definitions to the IPv4 IPAQENET INTERFACE statement.
2. Configure the SMCR parameter on the GLOBALCONFIG statement in the TCP/IP profile. The SMCR parameter includes the following subparameters:
   - PFID specifies the PCI Express (PCIe) function ID (PFID) value for an IBM 10GbE RoCE Express feature that this stack uses.

     You must code at least one PFID subparameter for this stack to use SMC-R, and two PFIDs per PNetID per stack for redundancy.
     - When the RoCE Express features operate in a dedicated RoCE environment, each RoCE Express feature must have a unique PFID value, but each TCP/IP stack that uses the RoCE Express feature specifies the same PFID value.
     - When the RoCE Express features operate in a shared RoCE environment, each TCP/IP stack that uses the same RoCE Express feature must have a unique PFID value, even if the TCP/IP stacks are defined on different LPARs.
   - PORTNUM specifies the 10GbE RoCE Express port number to use for each PFID.

     Configure each PFID to use only a single port. The port number can be 1 or 2; 1 is the default port number.
     - When the RoCE Express features operate in a dedicated RoCE environment, either port 1 or port 2 can be used for a particular 10GbE RoCE Express feature, but z/OS Communications Server cannot be configured to use both ports of a feature. For example, specifying `PFID 0018 PORTNUM 1` and `PFID 0018 PORTNUM 2`, even if specified on different TCP/IP stacks in the same LPAR, results in an error during 10GbE RoCE Express activation processing for the second port that is activated.
     - When the RoCE Express features operate in a shared RoCE environment, both port 1 and port 2 can be used simultaneously if the ports are associated with different PFID values. For example, assuming that PFID 0018 and PFID 0019 represent the same physical RoCE Express feature, you can specify `PFID 0019 PORTNUM 1` and `PFID 0018 PORTNUM 2` to use both ports.
   - MTU specifies the maximum transmission unit (MTU) to be used for this PFID. The default value is 1024. For more information, see "SMC-R RoCE maximum transmission unit" on page 46.
   - FIXEDMEMORY specifies the total amount of memory, in megabytes, that can be used for the staging and remote memory buffers.

     The default value is 256 MB.
   - TCPKEEPMININTERVAL specifies the minimum time interval, in seconds, for sending keepalive probes for TCP connections that use SMC-R protocols to exchange data.

     The default value is 300 seconds. For more information, see "TCP keepalive" on page 44.

The following GLOBALCONFIG statement defines two 10GbE RoCE Express features, PFID 0018 and PFID 0019. Port 2 is used on each feature, and the maximum amount of 64-bit private storage that can be used for SMC-R communications is 200 megabytes. The default values for both TCPKEEPMININTERVAL and MTU are used.

```
GLOBALCONFIG SMCR
    PFID 0018 PORTNUM 2
    PFID 0019 PORTNUM 2
    FIXEDMEMORY 200
```

For more information about these and other SMCR subparameters on the GLOBALCONFIG statement, see z/OS Communications Server: IP Configuration Reference.

3. (Optional) Configure the SMCR parameter on the IPAQENET and IPAQENET6 INTERFACE statements with the OSD channel path ID type (CHPIDTYPE OSD).

   Tip: SMCR is the default setting on the IPAQENET and IPAQENET6 INTERFACE statements for the OSD CHPID type.

   Guideline: If you enable Multipath and the equal-cost interfaces are associated with different IP subnets, enabling SMC for some of, but not all, the interfaces can cause unpredictable SMC usage. You must specify either SMCR or NOSMCR on all equal-cost interfaces.

4. Associate the interfaces with the appropriate subnet or prefix.
   - For an IPv4 interface to be eligible for SMC-R, you must configure a nonzero subnet mask on the INTERFACE statement in the TCP/IP profile.

     Result: SMC-R is used only between peers whose interfaces have the same subnet value.
   - For an IPv6 interface to be eligible for SMC-R, the interface must have at least one prefix that is associated with it.

     Rule: A prefix can be associated to an IPv6 interface in any of these ways:
     - A prefix received on a router advertisement message from an attached router
     - A prefix that is configured in OMPROUTE by using the PREFIX parameter on the IPV6_OSPF_INTERFACE, IPV6_RIP_INTERFACE, or IPV6_INTERFACE statement
     - A direct static prefix route that is configured over the interface on a ROUTE statement in a BEGINROUTES block in the TCP/IP profile

     Result: SMC-R is used only between peers whose IPv6 interfaces have at least one prefix in common.
5. (Optional) If you are using VLANs for your SMC-R communications, configure the VLANID parameter on the IPAQENET and IPAQENET6 INTERFACE statements for the OSD CHPID type. For more information, see "SMC-R VLANID usage" on page 25.
6. (Optional) If you have a server application that primarily uses short-lived TCP connections, you might want to avoid SMC-R rendezvous processing for TCP connections that are using that server port. Configure NOSMC on the PORT or PORTRANGE statement for the server port or ports that this server application uses. For more information, see z/OS Communications Server: IP Configuration Reference.

7. Start the IPAQENET and IPAQENET6 interfaces. When the first SMC-R capable OSD interface becomes active, z/OS Communications Server automatically starts all PFIDs that are defined in the GLOBALCONFIG statement, and associates the 10GbE RoCE Express interfaces with the OSD interfaces that have matching physical network IDs (PNet IDs). For more information about PNet IDs, see "SMC-R physical network considerations" on page 27.

What to do next

For information about how SMC-R interacts with other functions, see "SMC interactions with other z/OS Communications Server functions" on page 42.

For information about managing SMC-R communications, see "Managing SMC communications" on page 46.

Setting up the environment for Shared Memory Communications - Direct Memory Access

Before you configure Shared Memory Communications - Direct Memory Access (SMC-D), follow these steps to ensure that other components are configured.

Before you begin

Review "Configuration considerations for Shared Memory Communications" on page 24.

Procedure

Assign physical network ID (PNetID) values, and configure the values in the HCD for both the ISM devices and any OSA or HiperSockets devices that will use the ISM device for SMC-D communications.

Configuring Shared Memory Communications - Direct Memory Access

Use these steps to configure and begin to use Shared Memory Communications - Direct Memory Access (SMC-D).

Before you begin

See "Setting up the environment for Shared Memory Communications - Direct Memory Access."

Procedure

Perform the following steps to configure SMC-D:

1. If you are using IPv4 IPAQENET DEVICE, LINK, and HOME definitions, convert them to INTERFACE definitions. SMC-D processing is provided for only OSD interfaces that are configured with INTERFACE definitions. For more information about converting IPv4 IPAQENET DEVICE, LINK, and HOME definitions to INTERFACE definitions, see Steps for converting from IPv4 IPAQENET DEVICE, LINK, and HOME definitions to the IPv4 IPAQENET INTERFACE statement.
2. If you are using IPv4 IPAQIDIO DEVICE, LINK, and HOME definitions, convert them to INTERFACE definitions. SMC-D processing is provided for only HiperSockets interfaces that are configured with INTERFACE definitions. For more information about converting IPv4 IPAQIDIO DEVICE, LINK, and

HOME definitions to INTERFACE definitions, see Steps for converting from IPv4 IPAQIDIO DEVICE, LINK, and HOME definitions to the IPv4 IPAQIDIO INTERFACE statement.

3. Configure the SMCD parameter on the GLOBALCONFIG statement in the TCP/IP profile. The SMCD parameter includes the following subparameters:
   - FIXEDMEMORY specifies the total amount of memory, in megabytes, that can be used for the direct memory buffers. The default value is 256 MB.
   - TCPKEEPMININTERVAL specifies the minimum time interval, in seconds, for sending keepalive probes for TCP connections that use SMC-D protocols to exchange data. The default value is 300 seconds. For more information, see "TCP keepalive" on page 44.

   For more information about SMCD subparameters on the GLOBALCONFIG statement, see z/OS Communications Server: IP Configuration Reference.
4. (Optional) Configure the SMCD parameter on the IPAQENET and IPAQENET6 INTERFACE statements with the OSD channel path ID type (CHPIDTYPE OSD).

   Tip: SMCD is the default setting on the IPAQENET and IPAQENET6 INTERFACE statements for the OSD CHPID type.

   Guideline: If you enable Multipath and the equal-cost interfaces are associated with different IP subnets, enabling SMC for some of, but not all, the interfaces can cause unpredictable SMC usage. You must specify either SMCD or NOSMCD on all equal-cost interfaces.
5. (Optional) Configure the SMCD parameter on the IPAQIDIO and IPAQIDIO6 INTERFACE statements.

   Tip: SMCD is the default setting on the IPAQENET and IPAQENET6 INTERFACE statements.

   Guideline: If you enable Multipath and the equal-cost interfaces are associated with different IP subnets, enabling SMC for some of, but not all, the interfaces can cause unpredictable SMC usage. You must specify either SMCD or NOSMCD on all equal-cost interfaces.
6. Associate the interfaces with the appropriate subnet or prefix.
   - For an IPv4 interface to be eligible for SMC-D, you must configure a nonzero subnet mask on the INTERFACE statement in the TCP/IP profile.

     Result: SMC-D is used only between peers whose interfaces have the same subnet value.
   - For an IPv6 interface to be eligible for SMC-D, the interface must have at least one prefix that is associated with it.

     Rule: A prefix can be associated to an IPv6 interface in any of these ways:
     - A prefix that is received on a router advertisement message from an attached router
     - A prefix that is configured in OMPROUTE by using the PREFIX parameter on the IPV6_OSPF_INTERFACE, IPV6_RIP_INTERFACE, or IPV6_INTERFACE statement
     - A direct static prefix route that is configured over the interface on a ROUTE statement in a BEGINROUTES block in the TCP/IP profile

Result: SMC-D is used only between peers whose IPv6 interfaces have at least one prefix in common.

7. If you use VLANs for your SMC-D communications, configure the VLANID parameter on the IPAQENET and IPAQENET6 INTERFACE statements for the OSD CHPID type and on the IPAQIDIO and IPAQIDIO6 INTERFACE statements. For more information, see "VLANID considerations" on page 25.
8. If you have a server application that primarily uses short-lived TCP connections, you might avoid SMC-D rendezvous processing for TCP connections that are using that server port. Configure the NOSMC parameter on the PORT or PORTRANGE statement for the server port or ports that this server application uses. For more information, see z/OS Communications Server: IP Configuration Reference.
9. Start the IPAQENET and IPAQENET6 interfaces, or the IPAQIDIO and IPAQIDIO6 interfaces. When the first SMC-D capable OSD or HiperSockets interface becomes active for a given physical network ID (PNetID), z/OS Communications Server automatically looks for an available ISM device with a PNetID value that matches the PNetID value of the OSD or HiperSockets interface. If a matching ISM device is available, VTAM activates the ISM device and provides the associated PFID to the TCP/IP stack. For more information about PNetIDs, see "Physical network considerations" on page 26.

What to do next

For information about how SMC interacts with other functions, see "SMC interactions with other z/OS Communications Server functions."

For information about managing SMC communications, see "Managing SMC communications" on page 46.

SMC interactions with other z/OS Communications Server functions

SMC interacts with the following functions:

- "Sysplex distributor"
- "Security functions" on page 43
- "Intrusion detection services (IDS)" on page 43
- "TCP keepalive" on page 44
- "TCP application data transfer options" on page 45
- "Packet trace" on page 45
- "SMC-R RoCE maximum transmission unit" on page 46

Sysplex distributor

You can use Shared Memory Communications (SMC) with the sysplex distributor function with no additional configuration requirements. TCP connections are set up as normal through the sysplex distributor node, and the connection endpoints exchange SMC rendezvous information as described in "Rendezvous processing" on page 15. The sysplex distributor node examines information that is passed in the rendezvous exchange to select the optimum server application for SMC protocols. After the TCP connection is established to the server application, rendezvous processing continues to determine whether SMC communications are possible, and to establish an SMC link if necessary. After the TCP connection switches to SMC communications, the data does not flow through the sysplex distributor node, as shown in Figure 17 on page 43. This bypassing of the distributor node represents a performance improvement for the sysplex distributor

function when SMC protocols are used.

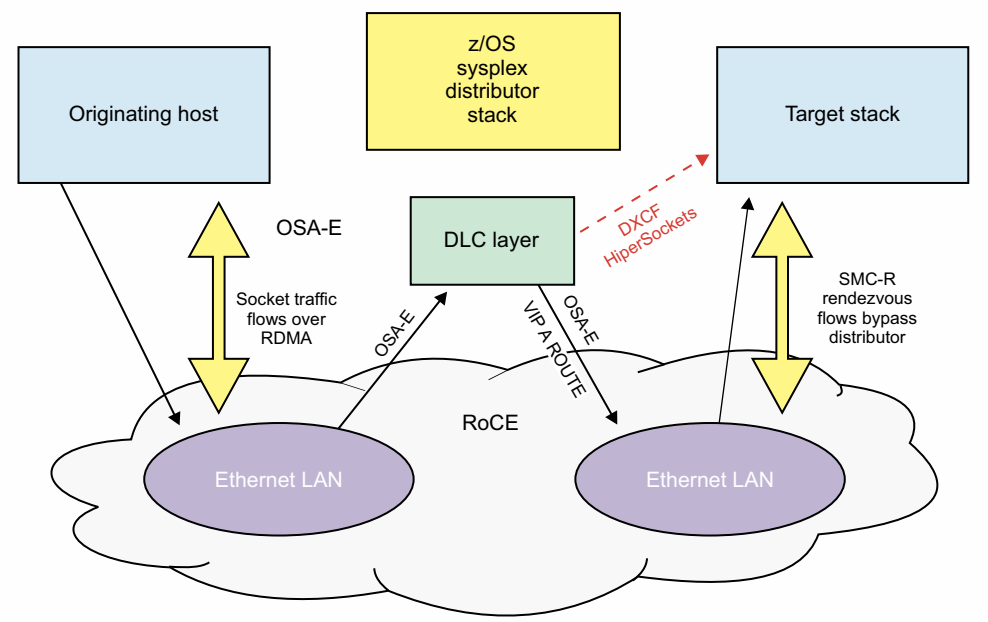


Figure 17. Sysplex distributor and SMC-R interaction

Security functions

You can use Application Transparent Transport Layer Security (AT-TLS) with SMC with no restriction. The negotiation of AT-TLS support for a TCP connection takes place after the SMC rendezvous exchange, and after that the encryption and decryption of the data occur as normal.

Generally, security functions that require TCP/IP to examine TCP packets cannot be used with SMC communications because data that is sent over SMC links is not converted into TCP packets. The following security functions do not interoperate with SMC:

- IPSec when the TCP connection requires tunneling
- IP filters when the filter would deny a packet for the TCP connection
- Multilevel security when the connection requires packet tagging (that is, when the source and destination zones are both SYSMULTI)

All of the above functions can be activated dynamically through profile changes, with the expectation that the change applies to current active TCP connections. If TCP connections are currently traversing SMC links when such a profile change is made, then the stack stops the TCP connections that are not compatible with the new security profiles.

Intrusion detection services (IDS)

Intrusion detection services (IDS) provides the following support:

- Scan detection and reporting
- Traffic regulation for TCP connections and UDP receive queues
- Attack detection, reporting, and prevention

The first two services involve checks that occur during TCP connection setup that do not interact directly with SMC communications.

The last service covers a range of checks. Most of the checks occur for inbound TCP packets, which means they are not applicable for SMC communications. The following two checks that are included in this service apply to TCP connections that traverse SMC links:

- TCP queue size events

  You can use IDS policy to detect when the send or receive queue for a TCP connection that traverses an SMC link becomes constrained because of the amount or age of the data on the queue. When a queue becomes constrained, you can reset the TCP connection or continue to monitor the condition until the queue is no longer constrained.

  Send or receive queues can be constrained for TCP connections that traverse SMC links:

  – The send queue is considered to be constrained when data is available to be sent but cannot be sent, or when data is stored into the peer remote memory buffer (RMB) or direct memory buffer (DMB) that is not acknowledged for more than 30 seconds.
  – The receive queue is considered to be constrained when data is available to be delivered but the application does not receive the data for more than 30 seconds.
  – When either queue becomes constrained, the TCP connections are monitored or stopped based on the IDS policy in effect.

- Global TCP stall events

  You can use IDS to detect attacks that are designed to consume system resources by creating many TCP connections and causing them to stall, making them unable to send data. A global stall condition is in effect when at least 50% of the active TCP connections are stalled and at least 1000 TCP connections are active. You can reset stalled connections, or continue to monitor the condition.

  TCP connections that traverse SMC links are considered for global TCP stall events. A TCP connection that traverses an SMC link is treated as a stalled connection when the TCB is write-blocked.

TCP keepalive

Some intermediate nodes (for instance, load balancers or firewalls) use data traffic as an indication that the TCP connection is still alive. If no data flows across the TCP path for a long enough period, the intermediate node might reset the connection. TCP keepalive processing periodically sends packets over the TCP connection to prevent the connection from being reset.

The rendezvous negotiations to use SMC communications occur over the TCP connection. After the decision to switch to SMC protocols is made, the TCP connection remains active, but only termination messages flow over the TCP connection as needed. The application socket data flows out of band by using RMDA or ISM protocols. Thus, a TCP connection that is using SMC can be viewed as using two paths:

- A TCP path that is used for non-data packets, including the initial three-way handshake packets, FIN packets, and RST packets.
- An SMC path that is used for data.

Because the TCP connection does not use the TCP path to exchange data packets, intermediate nodes might consider the connection to be idle for long periods. For TCP connections over SMC, keepalive processing must ensure that both the TCP path and the SMC path remain operational.

For traditional TCP connections, the time interval that is used to send keepalive probes is determined by using the following sequence:

1. The value of the TCP_KEEPALIVE setsockopt() option, if specified by the application
2. The value of the INTERVAL parameter on the TCPCONFIG statement

For a TCP connection that is traversing an SMC link, the time interval that is used to send keepalive probes on the SMC path is determined by using the same method because the SMC path is where the actual data flows. For these connections, however, use of this same method for the TCP path can generate excessive keepalive probe traffic, so a separate method is used to determine the keepalive time interval for the TCP path.

- For TCP connections that use SMC-R communications, this method uses the larger of the GLOBALCONFIG SMCR TCPKEEPMININTERVAL value, the TCPCONFIG INTERVAL value, and the TCP_KEEPALIVE setsockopt() value.
- For TCP connections that use SMC-D communications, this method uses the larger of the GLOBALCONFIG SMCD TCPKEEPMININTERVAL value, the TCPCONFIG INTERVAL value, and the TCP_KEEPALIVE setsockopt() value.

For example:

- SO_KEEPALIVE is specified by the application, TCPCONFIG INTERVAL is 120 minutes, and GLOBALCONFIG SMCR TCPKEEPMININTERVAL value is 5 minutes.

  In this case, the time interval for both the SMC-R path and the TCP path is 120 minutes.
- SO_KEEPALIVE is specified by the application, TCPCONFIG INTERVAL is 10 minutes, TCP_KEEPALIVE setsockopt() is specified by the application with a value of 5 minutes, and the GLOBALCONFIG SMCD TCPKEEPMININTERVAL value is 15 minutes.

  In this case, the time interval for the SMC-D path is 5 minutes, but the time interval for the TCP path is 15 minutes.

TCP application data transfer options

The SMC protocol is transparent to and fully compatible with TCP socket applications. A wide range of functions are available through the API interfaces that z/OS Communications Server provides. The use of SMC protocols for exchanging application socket data is not apparent to the applications. Thus, socket API functions such as MSGWAITALL, MSG_PEEK, Accept and Receive (ANR), and Urgent Data can still be used by the applications, even when SMC communications are used.

Packet trace

Packet trace provides a mechanism for capturing the contents of TCP packets as they are sent and received. Even though SMC does not create TCP packets for data that is sent over SMC links, the data is captured as part of packet trace processing. This data includes all TCP connection data that is sent across the SMC link, and any SMC-R Link Layer Control (LLC) messages that the TCP/IP stack generates to manage the link or the associated memory buffers.

For information about formatting the SMC data in the packet trace, see z/OS Communications Server: IP Diagnosis Guide.

SMC-R RoCE maximum transmission unit

RDMA protocols, including SMC-R, define a unique set of supported maximum transmission unit (MTU) sizes. SMC-R protocols support MTU sizes of 256, 512, 1024, 2048, and 4096 bytes, but z/OS Communications Server requests an MTU size of at least 1024 bytes. When an SMC-R link is initially established between two peer hosts, the MTU size is exchanged and negotiated to the lowest value for both hosts. The negotiated MTU size must account for transport headers and cyclic redundancy check (CRC) information that is used by the underlying RoCE protocols.

Guidelines:

- The default MTU value for Communications Server is 1024, which can be used for most z/OS application workloads.
- In some cases, such as streaming or bulk data transfer, you can improve throughput by using an MTU setting of 2048 or 4096. You can configure the MTU value on the PFID subparameter of the GLOBALCONFIG statement.
- If you set the MTU size to 2048 or 4096, you must also enable jumbo frames on all switches in the path for all peer hosts.
- Define the same MTU size for all PFIDs that are associated with the same physical network (PNetID).

Managing SMC communications

You can use the VARY command to manage your IBM 10GbE RoCE Express and ISM interfaces, and the Netstat command to display Shared Memory Communications (SMC) information. You can use various tools to monitor SMC information, and VTAM DISPLAY commands to display information about 10GbE RoCE Express and ISM interfaces. You can stop SMC at a stack-wide level.

Managing your 10GbE RoCE Express interfaces

The TCP/IP stack dynamically creates 10GbE RoCE Express interfaces for each configured PCI Express function ID (PFID). The stack activates all the configured 10GbE RoCE Express interfaces when the first SMC-R capable IPAQENET or IPAQENET6 interface is started. After the 10GbE RoCE Express interfaces are started, they remain active even when all SMC-R capable IPAQENET and IPAQENET6 interfaces are stopped. You can explicitly stop a 10GbE RoCE Express interface by using the VARY TCPIP,,STOP command. The name of the dynamically created 10GbE RoCE Express interfaces is in the form EZARIUT*pffff*, where *p* is the port number and *ffff* is the PFID.

Restriction: If you manually stop a 10GbE RoCE Express interface, you must later restart that interface by using the VARY TCPIP,,START command. The stack does not automatically restart the 10GbE RoCE Express interface when the next SMC-R capable interface is started.

In addition to stopping and starting the 10GbE RoCE Express interface, you can dynamically add or delete PFIDs from your TCP/IP profile by using the VARY TCPIP,,OBEYFILE command.

Steps for dynamically adding an IBM 10GbE RoCE Express interface:

Use these steps to dynamically add an IBM 10GbE RoCE Express interface.

Procedure

Perform the following steps:

1. Install and configure the 10GbE RoCE Express feature in the hardware configuration definition (HCD). Configuration includes the physical network ID (PNetID) for the 10GbE RoCE Express port. For more information, see "Physical network considerations" on page 26.
2. Add the new PCI Express function ID (PFID) to the GLOBALCONFIG SMCR parameter in the TCP/IP profile data set.

   Rule: In addition to the PFID that you are adding, you must also specify all currently configured PFIDs on the GLOBALCONFIG SMCR parameter. When you update the configured PFIDs on the GLOBALCONFIG SMCR parameter, you are completely replacing the configured PFID information.
3. Issue the VARY TCPIP,,OBEYFILE command and specify the updated TCP/IP profile data set.

Results

If any SMC-R capable IPAQENET and IPAQENET6 interfaces were ever active, the 10GbE RoCE Express interface that the added PFID represents is automatically started. Otherwise, the interface is started when the first SMC-R capable interface is started.

What to do next

For more information about dynamically updating the GLOBALCONFIG SMCR parameter, see z/OS Communications Server: IP Configuration Reference.

Steps for dynamically removing an IBM 10GbE RoCE Express interface:

Use these steps to dynamically remove an IBM 10GbE RoCE Express interface.

Procedure

Perform the following steps:

1. Issue the VARY TCPIP,,STOP command for the 10GbE RoCE Express interface to be deleted.

   Result: If no alternative SMC-R link exists for connections that are using this 10GbE RoCE Express interface, the connections are reset.
2. Remove the PCI Express function ID (PFID) value from the GLOBALCONFIG SMCR parameter in the TCP/IP profile data set.
3. Issue the VARY TCPIP,,OBEYFILE command and specify the updated TCP/IP profile data set.

What to do next

For more information about dynamically updating the GLOBALCONFIG SMCR parameter, see z/OS Communications Server: IP Configuration Reference.

Managing your ISM interfaces

The TCP/IP stack dynamically creates and activates an internal shared memory (ISM) interface for a specific physical network ID (PNetID) when both of the following conditions are true:

- The first SMC-D capable IPAQENET, IPAQENET6, IPAQIDIO, or IPAQIDIO6 interface is started for that PNetID.
- An ISM device with the same PNetID value is found.

After the ISM interface is started, it remains active even when all SMC-D capable interfaces are stopped. You can explicitly stop an ISM interface by using the VARY TCPIP,,STOP command. The name of the dynamically created ISM interfaces is in the form of EZAISM*xx*, where *xx* is a value from 01 to 32.

Restriction: If you manually stop an ISM interface, you must later restart that interface by using the VARY TCPIP,,START command. The stack does not automatically restart the ISM interface when the next SMC-D capable interface is started. If you stop and then restart the ISM interface, z/OS Communications Server might assign a different Peripheral Component Interconnect Express® (PCIe) function ID (PFID) to the ISM interface, depending on the availability of ISM devices that are associated with this PNetID.

Displaying SMC information

You can use the Netstat command and the DISPLAY TCPIP,,STOR command to display Shared Memory Communications (SMC) information.

For more information about these commands, see z/OS Communications Server: IP System Administrator's Commands.

Netstat ALL/-A report

You can use the Netstat ALL/-A report to determine whether a TCP connection is using SMC communications. You can filter the report by using the SMCID/-U filter and specifying an SMC-R link group ID, SMC-R link ID, or SMC-D link ID value as the filter. When a filter is specified, only those TCP connections that traverse the specified link group or link are displayed.

Netstat ALLConn/-a and Netstat COnn/-c reports

You can use the Netstat ALLConn/-a and Netstat COnn/-c reports to obtain TCP connection information. You can filter the reports by using the SMCID/-U filter and specifying an SMC-R link group ID, SMC-R link ID, or SMC-D link ID value as the filter. When a filter is specified, only those TCP connections that traverse the specified link group or link are displayed.

Netstat CONFIG/-f report

You can use the Netstat CONFIG/-f report to display the settings on the GLOBALCONFIG statement, which includes the SMCR and SMCD parameters and subparameters.

Netstat DEvlinks/-d report

You can use the Netstat DEvlinks/-d report to display the following information about interfaces:

- Whether an IPAQENET or IPAQENET6 interface is eligible for SMC-R, and if so, information about the associated 10GbE RoCE Express interfaces, also known as associated RNIC interfaces, that are in use.
- Whether an IPAQENET, IPAQENET6, IPAQIDIO, or IPAQIDIO6 interface is eligible for SMC-D, and if so, information about the associated internal shared memory (ISM) interface that is in use.

The physical network ID (PNetID) is also displayed, which can be useful in determining why 10GbE RoCE Express or ISM interfaces are not associated with the OSA or HiperSockets interface.

You can also use the Netstat DEvlinks/-d report to display information about SMC links and link groups:

- You can display the SMC-R links and SMC-R link groups that traverse a 10GbE RoCE Express interface, including the redundancy level for the link group as described in "SMC-R high availability considerations" on page 29.
- You can display the SMC-D links that traverse an ISM link.

To obtain information about SMC links and link groups, you must specify the SMC modifier on the Netstat command.

You can filter the Netstat report by using the SMCID/-U filter and specifying an SMC-R link ID or link group ID as the filter:

- When an SMC-R link ID is specified, information about that SMC-R link is displayed, in addition to information about the SMC-R link group that contains the link.
- When an SMC-R link group ID is specified, information about the SMC-R link group and all SMC-R links within the group is displayed.
- When an SMC-D link ID is specified, information about that SMC-D link is displayed.

You can display information about interfaces based on the PNetID value that is assigned to the interface by using the PNETID modifier on the Netstat command.

- To display all interfaces that have a PNetID value, specify PNETID=* as the modifier value.
- To display all interfaces that have a specific PNetID value, specify PNETID=*physical network ID* as the modifier value.

For more information, see z/OS Communications Server: IP System Administrator's Commands.

Netstat PORTList/-o report

You can use the Netstat PORTList/-o report to display the settings of the NOSMC and SMC parameters for the defined TCP port or range of ports.

Netstat STATS/-S report

You can use the Netstat STATS/-S report to display SMC-R and SMC-D usage statistics.

- In some cases, the statistics are a subset of the overall TCP statistics of the same name. For example, a value for the field `Current Established Connections` is displayed under `TCP Statistics`, `SMCR Statistics`, and `SMCD Statistics`. To determine the number of current connections that do not traverse an SMC link, subtract the total of SMC-R and SMC-D statistics from the total of TCP statistics.
- In other cases, the statistics represent information that is applicable to SMC-R or SMC-Dprocessing only. For instance, the field `Active SMC Links Opened` has no corresponding TCP statistics value.
- For information about which SMC statistics fit in which category in the Netstat STATS/-S report, see z/OS Communications Server: IP System Administrator's Commands.

DISPLAY TCPIP,,STOR output

You can use the DISPLAY TCPIP,,STOR command to display current SMC-R and SMC-D storage usage.

- SMC-R values are displayed for remote memory buffers (RMBs), denoted as `SMC-R RECV MEMORY`, and staging buffers, denoted as `SMC-R SEND MEMORY`. This storage is limited by the setting of the FIXEDMEMORY subparameter on the GLOBALCONFIG SMCR parameter. The SMC-R information is displayed only when the SMC-R function is enabled or was previously enabled for this TCP/IP stack.
- SMC-D values are displayed for direct memory buffers (DMBs), denoted as `SMC-D FIXEDMEMORY`. This storage is limited by the setting of the FIXEDMEMORY subparameter on the GLOBALCONFIG SMCD parameter. The SMC-D information is displayed only when the SMC-D function is enabled or was previously enabled for this TCP/IP stack.

Monitoring SMC information

z/OS Communications Server provides various tools that you can use to monitor Shared Memory Communications (SMC) information:

- "Network Management Interface"
- "SMF records" on page 51
- "SNMP" on page 51

Network Management Interface: Several TCP/IP callable NMI (EZBNMIFR) requests include information about SMC in general and specifics about IBM 10GbE RoCE Express and ISM interfaces:

- The GetConnectionDetail request provides information about active TCP connections, including SMC information for TCP connections that traverse SMC-R or SMC-D links.
- The GetGlobalStats request provides TCP/IP stack global statistics for IP, ICMP, TCP, UDP, SMC-R, and SMC-D processing.
- The GetIfs request provides TCP/IP stack interface attributes and IP addresses, including information about 10GbE RoCE Express and ISM interfaces.
- The GetProfile request provides profile information, including GLOBALCONFIG information for SMC-R and SMC-D.

In addition, the following NMI requests that are specific to SMC-R information are available:

- The GetRnics request, which provides interface statistics and VTAM tuning statistics that are related to 10GbE RoCE Express interfaces. This request

provides similar information to what is returned on the GetIfStats and GetIfExtendedStats requests for traditional interfaces.

- The GetSmcLinks request, which provides statistics about active SMC-R link groups and the SMC-R links within the link groups.

In addition, the following NMI requests that are specific to SMC-D information are available:

- The GetIsms request, which provides interface statistics that are related to ISM interfaces. This request provides similar information to what is returned on the GetIfStats and GetIfExtendedStats requests for traditional interfaces.
- The GetIsmLinks request, which provides statistics about active SMC-D links.

For specifics about these TCP/IP callable NMI requests, see z/OS Communications Server: IP Programmer's Guide and Reference.

SMF records: Several SMF 119 records include information about SMC-R in general and specifics about IBM 10GbE RoCE Express interfaces. In addition, SMF TYPE 119 records that are specific to SMC-R processing are available:

- The SMC-R Link State Start (subtype 42) and SMC-R Link State End (subtype 43) SMF records notify the user when an SMC-R link is activated or deactivated. These SMF records serve a similar purpose for SMC-R links as the TCP Connection Start and TCP Connection End records serve for TCP connections.
- The SMC-R Link Group Statistics SMF record (subtype 41) provides statistics for all active SMC-R link groups on an interval basis. This SMF record includes information pertinent to both SMC-R link groups and the individual SMC-R links that comprise the link group.
- The RNIC Interface Statistics SMF record (subtype 44) provides interface statistics for 10GbE RoCE Express interfaces. This SMF record serves the same purpose for 10GbE RoCE Express interfaces that the Interface Statistics SMF record (subtype 6) serves for other interfaces.

For more information about type 119 SMF records, see z/OS Communications Server: IP Programmer's Guide and Reference.

SNMP: The Simple Network Management Protocol (SNMP) TCP/IP subagent provides Shared Memory Communications over RDMA (SMC-R) information, such as SMC-R eligibility and the associated physical network ID (PNetID) for IPAQENET and IPAQENET6 interfaces. SNMP also reports basic information about 10GbE RoCE Express interfaces. The following SNMP MIB tables contain the information:

- ibmTcpipMvsIfTable
- ibmTcpipMvsPortTable

All the MIB objects that are supported by Communications Server functions are listed in the MIB objects appendix in z/OS Communications Server: IP System Administrator's Commands.

VTAM displays and tuning statistics

When an IBM 10GbE RoCE Express or internal shared memroy (ISM) interface is first started, VTAM dynamically creates a transport resource list element (TRLE) to represent it.

- For an 10GbE RoCE Express interface, the TRLE name is in the form of IUT*ppppp*, where *p* is the port number and *ffff* is the PCI-Express function ID (PFID). For example, if you specify `GLOBALCONFIG SMCR PFID 0018 PORTNUM 1`, the TRLE name is IUT10018.
- For an ISM interface, the TRLE name is in the form of IUT0*ffff*, where *ffff* is the PFID that is associated with the ISM device that VTAM selects to use with this physical network. For example, if the PFID value is 0024, the TRLE name is IUT00024.

You can use the VTAM DISPLAY TRL and DISPLAY ID commands to display information about the TRLE representation of the 10GbE RoCE Express or ISM interface, including information about the physical network ID (PNetID), and which TCP stacks use the interface.

Tip: For a 10GbE RoCE Express TRLE, use the presence of a virtual function number (VFN) in the DISPLAY TRL or DISPLAY ID command output to determine whether the RoCE Express feature operates in a shared RoCE environment. A VFN is present in a shared environment and absent in a dedicated environment.

VTAM tuning statistics are managed differently for 10GbE RoCE Express interfaces and ISM interfaces:

- VTAM collects tuning statistics for 10GbE RoCE Express interfaces when requested by using the TNSTAT start option or the MODIFY TNSTAT command. Tuning statistics that represent processing at a 10GbE RoCE Express interface level and statistics at a user or TCP/IP stack level are both maintained. The TCP/IP stack level statistics are also provided on the GetRnics request. For more information, see "Network Management Interface" on page 50.
- ISM interfaces are not affected by the MODIFY TNSTAT command or the TNSTAT start option. VTAM collects a minimal set of tuning statistics for the ISM interface, and these statistics are included on the Netstat DEvlinks/-d report and the GetIsms request. For more information, see "Network Management Interface" on page 50.

For more information about the VTAM commands, see z/OS Communications Server: SNA Operation. For more information about gathering tuning statistics, see z/OS Communications Server: SNA Network Implementation Guide.

Stopping SMC-R

You can stop Shared Memory Communications over RDMA (SMC-R) at a stack-wide level.

Procedure

Perform the following steps to stop SMC-R:

1. Modify the GLOBALCONFIG statement in the TCP/IP profile data set to include the NOSMCR parameter.
2. Issue the VARY TCPIP,,OBEYFILE,*profile_data_set* command.

Results

The TCP/IP stack does not immediately stop all existing SMC-R processing after the VARY TCPIP,,OBEYFILE command is processed. Existing TCP connections that are using existing SMC-R links are unaffected and continue to use SMC-R communications until they end or are stopped. However, no new SMC-R link

groups or links are created, and no TCP connections that are established after this point use the existing SMC-R links.

What to do next

When you are restarting SMC-R after a stop, the previous SMCR parameter settings are used when they are not explicitly configured in the OBEYFILE data set. For more information about dynamically updating the GLOBALCONFIG SMCR parameter, see z/OS Communications Server: IP Configuration Reference.

Stopping SMC-D

You can stop Shared Memory Communications - Direct Memory Access (SMC-D) at a stack-wide level.

Procedure

1. Modify the GLOBALCONFIG statement in the TCP/IP profile data set to include the NOSMCD parameter.
2. Issue the VARY TCPIP,,OBEYFILE,*profile_data_set* command.

Results

The TCP/IP stack does not immediately stop all existing SMC-D processing after the VARY TCPIP,,OBEYFILE command is processed. Existing TCP connections that are using existing SMC-D links are unaffected and continue to use SMC-D communications until SMC-D links end or are stopped. However, no new SMC-D links are created, and TCP connections that are established after this point do not use the existing SMC-D links.

What to do next

When you restart SMC-D after a stop, the previous SMCD parameter settings are used if they are not explicitly configured in the OBEYFILE data set. For more information about dynamically updating the GLOBALCONFIG SMCD parameter, see z/OS Communications Server: IP Configuration Reference.

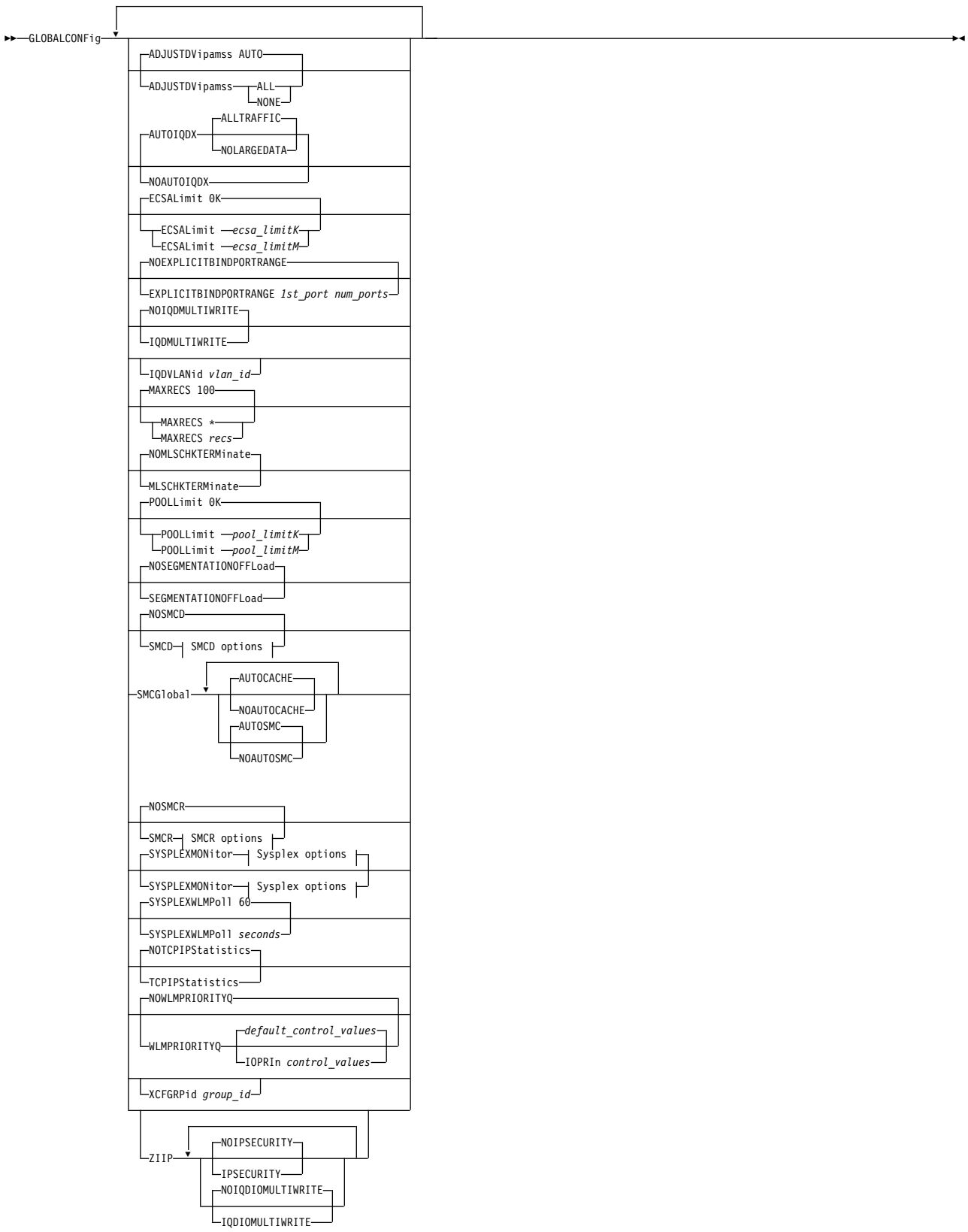
Chapter 3. IP Configuration Reference

GLOBALCONFIG statement

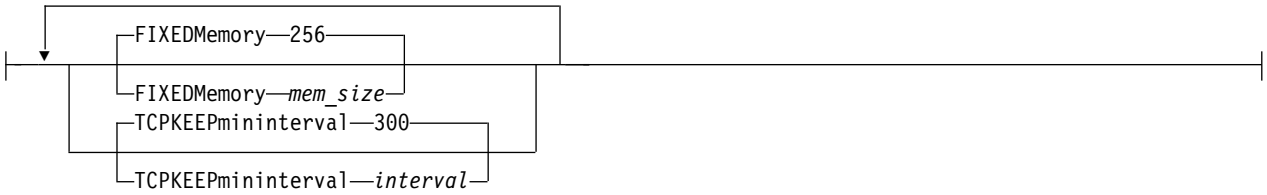
Use the GLOBALCONFIG statement to pass global configuration parameters to TCP/IP.

Syntax

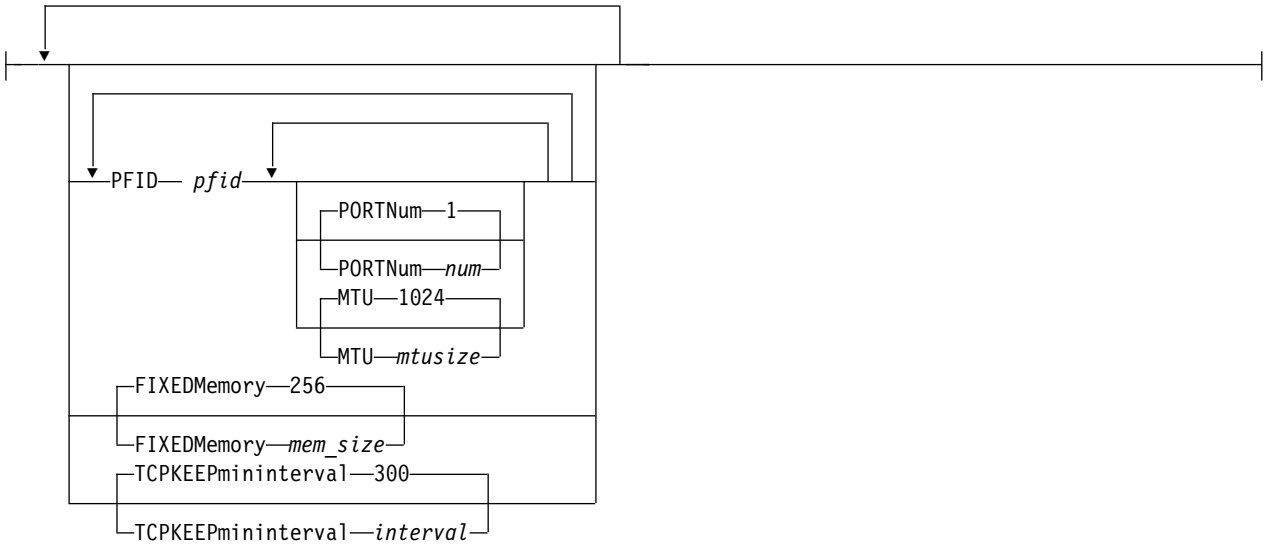
Tip: Specify the parameters for this statement in any order.


GLOBALCONFig
ADJUSTDVipamss AUTO
ADJUSTDVipamss
ALL
NONE
AUTOIQDX
ALLTRAFFIC
NOLARGEDATA
NOAUTOIQDX
ECSALimit 0K
ECSALimit ecsa_limitK
ECSALimit ecsa_limitM
NOEXPLICITBINDPORTRANGE
EXPLICITBINDPORTRANGE 1st_port num_ports
NOIQDMULTIWRITE
IQDMULTIWRITE
IQDVLANid vlan_id
MAXRECS 100
MAXRECS *
MAXRECS recs
NOMLSCHKTERMinate
MLSCHKTERMinate
POOLLimit 0K
POOLLimit pool_limitK
POOLLimit pool_limitM
NOSEGMENTATIONOFFLoad
SEGMENTATIONOFFLoad
NOSMCD
SMCD
SMCD options
SMCGlobal
AUTOCACHE
NOAUTOCACHE
AUTOSMC
NOAUTOSMC
NOSMCR
SMCR
SMCR options
SYSPLEXMONitor
Sysplex options
SYSPLEXMONitor
Sysplex options
SYSPLEXWLMPoll 60
SYSPLEXWLMPoll seconds
NOTCPIPStatistics
TCPIPStatistics
NOWLMPRIORITYQ
WLMPRIORITYQ
default_control_values
IOPRIn control_values
XCFGRPid group_id
ZIIP
NOIPSECURITY
IPSECURITY
NOIQDIOMULTIWRITE
IQDIOMULTIWRITE

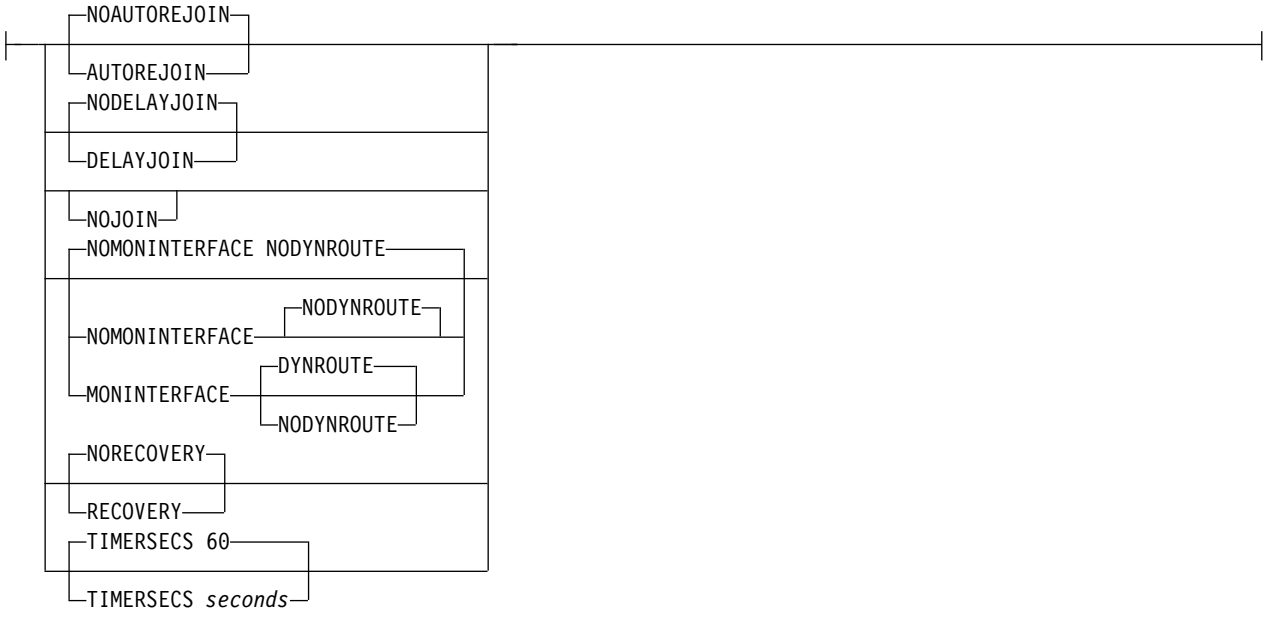
SMCD options:



SMCR options:



Sysplex options:



Parameters

ADJUSTDVIPAMSS AUTO | ALL | NONE

Specifies subparameters to control whether TCP/IP changes the Maximum Segment Size (MSS) that is advertised for a TCP connection. Connections that use VIPAROUTE to forward Sysplex Distributor packets add a Generic Routing Encapsulation (GRE) header to the packet. The addition of a GRE header increases the packet size and can cause IP fragmentation between the distributor and the target stack. To avoid this fragmentation, the length of the GRE header can be subtracted from the MSS that TCP connections advertise at connection establishment. Changes to ADJUSTDVIPAMSS affect only the new connections.

AUTO
Indicates that TCP/IP automatically adjusts the MSS to accommodate the length of a GRE header. For inbound connections on a target stack, the MSS is adjusted if the destination address is a distributed DVIPA and VIPAROUTE is being used. For outbound connections on a target stack, the MSS is adjusted if the source IP address is a distributed DVIPA. This is the default value.

ALL Indicates that TCP/IP adjusts the MSS for connections that use a DVIPA as the local IP address, whether the DVIPA is distributed or not.

NONE
Indicates that TCP/IP does not adjust the MSS for any connections.

AUTOIQDX | NOAUTOIQDX

Specifies whether to use dynamic Internal Queued Direct I/O extensions (IQDX) interfaces for connectivity to the intraensemble data network.

See "Steps for modifying" on page 74 for details about changing this parameter while the TCP/IP stack is active. See z/OS Communications Server: IP Configuration Guide for information about the intraensemble data network and the dynamic IQDX function.

NOAUTOIQDX
Do not use dynamic IQDX interfaces.

AUTOIQDX
Use dynamic IQDX interfaces when an IQD CHPID has been configured with the Internal Queued Direct I/O extensions (IQDX) function. This value is the default value.

ALLTRAFFIC
Use IQDX interfaces for all eligible outbound traffic on the intraensemble data network. This value is the default value.

NOLARGEDATA
Do not use IQDX interfaces for outbound TCP socket data transmissions of length 32KB or larger. Use IQDX interfaces for all other eligible outbound traffic. See z/OS Communications Server: IP Configuration Guide for more information.

ECSALIMIT *ecsalimit* **K | M**

Specifies the maximum amount of extended common service area (ECSA) that TCP/IP can use. This limit can be expressed as a number followed by a K (which represents 1024 bytes), or a number followed by an M (which represents 1048576 bytes). If the K suffix is used, *ecsalimit* must be in the range 10240K and 2096128K inclusive or 0. If the M suffix is used, *ecsalimit* must be

in the range 10M and 2047M inclusive or 0. The default is no limit, and it can be specified as 0 K or 0 M. The minimum value for ECSALIMIT and POOLLIMIT is not allowed to be set to a value if the current storage in use would be greater than or equal to 80% of that value (for example, not allowed to set it such that there is an immediate storage shortage).

ECSALIMIT ensures that TCP/IP does not overuse common storage. It is intended to improve system reliability by limiting TCP/IP's storage usage. The limit must account for peak storage usage during periods of high system activity or TCP/IP storage abends might occur. The limit does not include storage used by communications storage manager (CSM). CSM ECSA storage is managed independently of the TCP/IP ECSALIMIT. See z/OS Communications Server: SNA Network Implementation Guide for more information about CSM.

Specifying a nonzero ECSALIMIT enables warning messages EZZ4360I, EZZ4361I, and EZZ4362I to appear if a storage shortage occurs.

EXPLICITBINDPORTRANGE | NOEXPLICITBINDPORTRANGE

NOEXPLICITBINDPORTRANGE
Indicates that this stack does not participate in the allocation of ports from a pool of ports. The ports in the pool are guaranteed to be unique across the sysplex in that they are allocated to only one requestor in the sysplex at any one time, when processing an explicit bind() of a TCP socket to the IPv4 INADDR_ANY address, or to the IPv6 unspecified address (in6addr_any), and port 0.

EXPLICITBINDPORTRANGE
Indicates that this stack participates in the allocation of ports from a pool of ports guaranteed to be unique across the sysplex, when processing an explicit bind() of a TCP socket to the IPv4 INADDR_ANY address, or to the IPv6 unspecified address (in6addr_any), and port 0. This parameter also designates the range of ports that defines that pool. This parameter defines the range used by all stacks participating in EXPLICITBINDPORTRANGE port allocation processing throughout the sysplex. The most recently processed profile or OBEYFILE command that specifies EXPLICITBINDPORTRANGE defines the range for the sysplex.

Use this parameter so that you can specify distributed DVIPAs as the source IP address on DESTINATION or JOBNAME rules in a SRCIP block. See SRCIP statement.

1st_port
The starting port for the range of ports. The *1st_port* value is in the range 1024 - 65535. The sum of the *1st_port* value plus the *num_ports* value minus 1 cannot exceed 65535.

num_ports
The number of ports in the range. The *num_ports* value is in the range 1 - 64512. The sum of the *1st_port* value plus the *num_ports* value minus 1 cannot exceed 65535.

Guidelines:

- All TCP/IP stacks in the sysplex that participate in EXPLICITBINDPORTRANGE processing should have the same port range specified. To ensure this, specify the GLOBALCONFIG

EXPLICITBINDPORTRANGE statement in a file that is specified in an INCLUDE statement in the TCP profiles data set of all the participating stacks.

- The port range defined on the EXPLICITBINDPORTRANGE parameter should not overlap any existing port reservations of any TCP/IP stacks in the sysplex. Any reserved ports that are within the EXPLICITBINDPORTRANGE range are excluded from the EXPLICITBINDPORTRANGE port pool, effectively making the pool smaller.
- The EXPLICITBINDPORTRANGE port range must be large enough to accommodate all applications in the sysplex that might issue explicit bind() calls for the IPv4 INADDR_ANY address, or for the IPv6 unspecified address (in6addr_any), and port 0.
- If additional TCP/IP stacks or systems are introduced into the sysplex, the extent of the port range defined by EXPLICITBINDPORTRANGE should be re-evaluated.
- If the size of the port range defined by the EXPLICITBINDPORTRANGE parameter is too large, there are fewer ports available for local ephemeral port allocation.
- If you specify the EXPLICITBINDPORTRANGE parameter in a sysplex that contains pre-V1R9 TCP/IP stacks, each distributor, backup, and target TCP/IP stack of a distributed SYSPLEXPORTS DVIPA that is configured as a source IP address on a SRCIP profile statement must have one of the following characteristics:
  - Run on a V1R9 or later system.
  - Use the PORTRANGE profile statement on the pre-V1R9 stacks to reserve the ports that are configured on the V1R9 or later stacks with the EXPLICITBINDPORTRANGE parameter.

  Failure to meet these characteristics can result in connection failures because unique ports assignments are no longer be assured throughout the sysplex for a SYSPLEXPORTS distributed DVIPA; the same port value could be assigned from the following pools:
  - The DVIPA-specific pool by a pre-V1R9 system
  - The EXPLICITBINDPORTRANGE pool by a V1R9 or later system

Restriction: In a common INET (CINET) environment, this parameter is accepted, but the EXPLICITBINDPORTRANGE function is supported in a limited set of conditions only. It is supported when CINET is managing one stack only on the system or when the affected application has established stack affinity. Otherwise, results can be unpredictable.

IQDMULTIWRITE | NOIQDMULTIWRITE

Specifies whether HiperSockets interfaces should use multiple write support. HiperSockets multiple write might reduce CPU usage and might provide a performance improvement for large outbound messages that are typically generated by traditional streaming workloads such as file transfer, and interactive web-based services workloads such as XML or SOAP. This parameter applies to all HiperSockets interfaces, including IUTIQDIO and IQDIOINTF6 interfaces created for Dynamic XCF.

Restriction: HiperSockets multiple write is effective only on an IBM System z10™ or later and when z/OS is not running as a guest in a z/VM® environment.

See the modifying information in this topic for details about changing this parameter while the TCP/IP stack is active. See the HiperSockets multiple

write information in z/OS Communications Server: IP Configuration Guide for more information about HiperSockets multiple write support.

NOIQDMULTIWRITE
HiperSockets interfaces do not use the multiple write support. This is the default.

IQDMULTIWRITE
HiperSockets interfaces do use the multiple write support.

IQDVLANID *vlan_id*
Specifies a VLAN ID to be used when HiperSockets (iQDIO) connectivity is used for dynamic XCF support. VLAN IDs are used to partition communication across HiperSockets. Stacks on the same CPC using the same HiperSockets CHPID that use the same VLAN ID can establish communications; stacks on the same CPC using the same HiperSockets CHPID that use different VLAN IDs cannot.

The specified value, *vlan_id*, is used for both IPv4 and IPv6 DYNAMICXCF HiperSockets connectivity. This parameter is intended to be used in conjunction with the GLOBALCONFIG XCFGRPID parameter to support subplexing.

Subplexing enables TCP/IP participation in a Sysplex to be partitioned into subsets based on the XCFGRPID value. When using subplexing, TCP/IP stacks with the same XCFGRPID value should specify the same IQDVLANID value. Stacks with different XCFGRPID values should have different IQDVLANID values. If you have stacks in the default subplex (that is, stacks that do not specify an XCFGRPID value) that use the same HiperSockets CHPID as stacks within a non-default subplex (an XCFGRPID value was specified), then the stacks in the default subplex should specify an IQDVLANID value that is different from the other IQDVLANID values specified by the other non-default subplex stacks that use the same HiperSockets CHPID.

Restriction: The IQDVLANID parameter can be specified only in the initial profile.

Valid VLAN IDs are in the range 1 - 4094. For more information about VLANs and Hipersockets see z/OS Communications Server: IP Configuration Guide.

MAXRECS
Specifies the maximum number of records to be displayed by the DISPLAY TCPIP,,NETSTAT operator command. The term *records* refers to the number of entries displayed on each report. For example, for the connection-related reports, a record is a TCP connection or listener, or a UDP endpoint. This configured value is used when the MAX parameter is not explicitly specified on the command. The default value is 100. If the number of output lines exceeds the maximum number of lines for a multi-line Write to Operator (WTO), the report output is truncated. See the information about the Display TCPIP,,NETSTAT command in z/OS Communications Server: IP System Administrator's Commands for more details about the command.

* A value of asterisk (*) specifies that all records are to be displayed.

recs This value specifies the number of records to be displayed. The valid range is 1 - 65535.

MLSCHKTERMINATE | NOMLSCHKTERMINATE

NOMLSCHKTERMINATE
Specifies that the stack should remain active after writing an

informational message when inconsistent configuration information is discovered in a multilevel-secure environment.

Informational message EZD1217I is written to the system console summarizing the number of problems found. Additional informational messages between EZD1219I and EZD1234I are written to the job log for each configuration inconsistency found.

This is the default value.

MLSCHKTERMINATE
Specifies that the stack should be terminated after writing an informational message when inconsistent configuration information is discovered in a multilevel-secure environment.

Informational message EZD1217I is written to the system console summarizing the number of problems found. Additional informational messages between EZD1219I and EZD1234I are written to the job log for each configuration inconsistency found.

POOLLIMIT *pool_limit* **K | M**
Specifies the maximum amount of authorized private storage that TCP/IP can use within the TCP/IP address space. This limit can be expressed as a number followed by a K (which represents 1024 bytes), or a number followed by an M (which represents 1048576 bytes). If the K suffix is used, *pool_limit* must be in the range 10240K and 2096128K inclusive or 0. If the M suffix is used, *pool_limit* must be in the range 10M and 2047M inclusive or 0. The default is no limit, and it can be specified as 0K or 0M. The minimum value for ECSALIMIT and POOLLIMIT is not allowed to be set to a value if the current storage in use would be greater than or equal to 80% of that value (for example, not allowed to set it such that there is an immediate storage shortage).

POOLLIMIT ensures that TCP/IP does not overuse its authorized private storage. Most systems can use the default POOLLIMIT (no limit). Systems with limited paging capacity can use POOLLIMIT to help limit TCP/IP storage usage. If the limit is used, it must account for peak storage usage during periods of high system activity or TCP/IP storage abends might occur.

POOLLIMIT can be higher than the REGION size on the TCP/IP start procedure because POOLLIMIT applies to authorized storage, whereas REGION applies to unauthorized storage. Specifying a nonzero POOLLIMIT enables warning messages EZZ4364I, EZZ4365I, and EZZ4366I to appear if a storage shortage occurs.

SEGMENTATIONOFFLOAD | NOSEGMENTATIONOFFLOAD
Specifies whether the stack should offload TCP segmentation for IPv4 packets to OSA-Express features. TCP segmentation offload support transfers the overhead of segmenting outbound data into individual TCP packets to QDIO-attached OSA-Express devices whose features that support this function. Offloading segmentation of streaming-type workloads reduces CPU use and increases throughput. This parameter is ignored for OSA-Express features that do not support segmentation offload.

Guideline: The support for specifying IPv4 segmentation offload on the GLOBALCONFIG profile statement has been deprecated. The parameters are still supported on the GLOBALCONFIG statement, but the support for specifying these parameters on the GLOBALCONFIG statement will be dropped in a future release. It is recommended to specify these parameters on the IPCONFIG profile statement instead.

Rule: The SEGMENTATIONOFFLOAD and NOSEGMENTATIONOFFLOAD parameters specified on the IPCONFIG statement override the equivalent parameters specified on the GLOBALCONFIG statement.

See the Modifying topic for information about changing this parameter while the TCP/IP stack is active. See TCP segmentation offload information in z/OS Communications Server: IP Configuration Guide for more information about TCP segmentation offload support.

NOSEGMENTATIONOFFLOAD
TCP segmentation is performed by the TCP/IP stack. This is the default.

SEGMENTATIONOFFLOAD
TCP segmentation is offloaded to the OSA-Express feature.

SMCD | NOSMCD
Specifies whether this stack uses Shared Memory Communications - Direct Memory Access (SMC-D). For more information about SMC-D, see in z/OS Communications Server: IP Configuration Guide.

NOSMCD
Specifies that this stack should not use SMC-D communications. This is the default setting.

SMCD
Specifies that this stack should use SMC-D communications. You can use this parameter to define operational characteristics for SMC-D communications.

Result: The AUTOCACHE and AUTOSMC monitoring functions are started if SMCGLOBAL AUTOCACHE and AUTOSMC are configured, either by default or by being explicitly specified.

If you specify the SMCD parameter without any subparameters, you get one of the following results:

- If you specify the SMCD parameter for the first time, the FIXEDMEMORY and TCPKEEPMININTERVAL subparameters are set to default values.
- If you previously specified the SMCD parameter with subparameters, TCP/IP retains the knowledge of the subparameter settings, even if SMC-D processing is stopped by issuing the VARY TCPIP,,OBEYFILE command with a data set that contains a GLOBALCONFIG NOSMCD parameter. Therefore, a subsequent specification of a GLOBALCONFIG SMCD profile statement resumes SMC-D processing with the previous subparameter settings.

FIXEDMEMORY *mem_size*
Specifies the maximum amount of 64-bit storage that the stack can use for the receive buffers that are required for SMC-D communications. The *mem_size* value is an integer in the range 30 - 9999, and represents the maximum storage in megabytes of data. The default value is 256 megabytes.

TCPKEEPMININTERVAL *interval*
This interval specifies the minimum interval that TCP keepalive packets are sent on the TCP path of an SMC-D link.

Rules:

- If a keepalive interval is also specified on the INTERVAL parameter of the TCPCONFIG statement or is set for a specific SMC-D link socket by the TCP_KEEPALIVE setsockopt() option, the largest of the three interval values is used.
- The valid range for this interval is 0-2147460 seconds, and the default value is 300 seconds.
- A value of 0 disables TCP keepalive probe packets on the TCP path of an SMC-D link.
- The SO_KEEPALIVE setsockopt() option must be set to use keepalive processing.

Result: The TCPKEEPMININTERVAL setting has no effect on keepalive processing for the SMC-D path of an SMC-D link.

For more information about TCP keepalive processing for the TCP path and the SMC-D path of SMC-D links, see TCP keepalive in z/OS Communications Server: IP Configuration Guide.

SMCGLOBAL

Specifies global settings for Shared Memory Communications (SMC). SMC includes Shared Memory Communications over Remote Direct Memory Access (RDMA), or SMC-R, for external data network communications and Shared Memory Communications - Direct Memory Access (SMC-D). For more information about SMC-R and SMC-D, see Shared Memory Communications in z/OS Communications Server: IP Configuration Guide.

AUTOCACHE | NOAUTOCACHE

Specifies whether this stack caches unsuccessful attempts to use SMC communication. Use SMCGLOBAL AUTOCACHE to prevent the overhead of persistent attempts to establish a TCP connection to a specific destination IP address over SMC if previous attempts to the same destination failed.

NOAUTOCACHE

Specifies that this stack does not cache unsuccessful attempts to create an SMC-R or SMC-D link and that existing SMC cache entries are cleared.

AUTOCACHE

Specifies that this stack caches unsuccessful attempts to create an SMC-R or SMC-D link per destination IP address. Subsequent TCP connections to the same destination bypass the use of SMC while the IP address is cached. To clear this cache, specify the NOAUTOCACHE subparameter. Cached entries remain in effect for approximately 20 minutes. AUTOCACHE is the default setting. The AUTOCACHE function is started only when you enable SMC. For more information about enabling SMC, see the description of the GLOBALCONFIG SMCR and SMCD parameters.

AUTOSMC | NOAUTOSMC

Specifies whether this stack monitors inbound TCP connections to dynamically determine whether SMC is beneficial for a local TCP server application. Results of this monitoring influence whether TCP connections to a particular server or port use SMC. AUTOSMC monitoring ensures that TCP connections use the most appropriate

communications protocol, either TCP or SMC. You can use the Netstat ALL/-A command to monitor the results of this dynamic monitoring and SMC enablement or disablement. For more information about the Netstat ALL/-A command, see Netstat ALL/-A report in z/OS Communications Server: IP System Administrator's Commands.

Guideline: Configuration of either SMC or NOSMC on the PORT or PORTRANGE statement overrides configuration of the AUTOSMC monitoring function for particular servers. For more information, see "PORT statement" on page 144 and "PORTRANGE statement" on page 153.

NOAUTOSMC
Specifies that this stack does not monitor inbound TCP connections to determine whether the connections can benefit from using SMC.

AUTOSMC
Specifies that this stack monitors inbound TCP connections to determine whether the connections can benefit from using SMC. AUTOSMC is the default setting. The AUTOSMC monitoring function is started only when you enable SMC. For more information about enabling SMC, see the description of the GLOBALCONFIG SMCR and SMCD parameters.

SMCR | NOSMCR
Specifies whether this stack uses Shared Memory Communications over Remote Direct Memory Access (RDMA), or SMC-R, for external data network communications. For more information about SMC-R, see Shared Memory Communications over Remote Direct Memory Access in z/OS Communications Server: IP Configuration Guide.

NOSMCR
Specifies that this stack should not use SMC-R for external data network communications. This is the default setting.

SMCR
Specifies that this stack should use SMC-R for external data network communications. Use this parameter to define the IBM 10GbE RoCE Express features that this stack should use for SMC-R communications. You can use this parameter to define additional operational characteristics for SMC-R communications.

Result: If at least one PFID is defined, the AUTOCACHE and AUTOSMC monitoring functions are started if SMCGLOBAL AUTOCACHE and AUTOSMC are configured, either by default or by being explicitly specified.

If you specify the SMCR parameter without any subparameters, you get one of the following results:

- If this is the first time that you specify the SMCR parameter, the following results occur:
  - No Peripheral Component Interconnect Express (PCIe) function IDs are defined.
  - FIXEDMEMORY and TCPKEEPMININTERVAL subparameters are set to default values.
- If you previously specified the SMCR parameter with subparameters, TCP/IP retains the knowledge of the subparameter

settings, even if SMC-R processing is stopped by issuing the VARY TCPIP,,OBEYFILE command with a data set that contains a GLOBALCONFIG NOSMCR parameter. Therefore, a subsequent specification of a GLOBALCONFIG SMCR profile statement resumes SMC-R processing with the previous subparameter settings.

PFID *pfid*

Specifies the Peripheral Component Interconnect Express (PCIe) function ID (PFID) value for a 10GbE RoCE Express feature that this stack uses. A *pfid* is a 2-byte hexadecimal value in the range 0 - 0FFF that identifies this TCP/IP stack's representation of a 10GbE RoCE Express feature.

Rules:

- You must code at least one PFID subparameter for this stack to use SMC-R communications.
- You can specify a maximum of 16 PFID subparameter values on the SMCR parameter.
- The value for each PFID and PORTNUM pair must be unique.
- When the RoCE Express feature operates in a shared RoCE environment, you cannot simultaneously activate a 10GbE RoCE Express feature that uses the same PFID value from different TCP/IP stacks within the same logical partition (LPAR).

PORTNUM *num*

Specifies the 10GbE RoCE Express port number to use for a particular PFID. Configure each PFID to use only a single port. The port number can be 1 or 2; 1 is the default value.

Rules:

- If the 10GbE RoCE Express feature operate 10Gbe RoCE Express features in a dedicated RoCE environment, you can activate either port 1 or port 2 but not both simultaneously for an individual PFID value. If PORTNUM 1 and PORTNUM 2 definitions for the same PFID value are created, the port that is first activated is used.
- If the 10GbE RoCE Express feature operates in a shared RoCE environment, you can use both port 1 and port 2 on an individual RNIC adapter, but the PFID value that is associated with each port must be different. You cannot simultaneously activate PORTNUM 1 and PORTNUM 2 definitions for the same PFID value.

  For example, if PFID 0013 and PFID 0014 are both defined in HCD to represent the RNIC adapter with PCHID value 0140, you can configure `PFID 0013 PORT 1 PFID 0014 PORT 2` to use both ports on the RNIC adapter. However, if you specify `PFID 0013 PORT 1 PFID 0013 PORT 2`, only the first port that is activated is used.

MTU *mtusize*

Specifies the maximum transmission unit (MTU) value to be used for a particular PFID. The MTU value can be 1024, 2048, or 4096. The default value is 1024 and can be used for most workloads. If you set the MTU size to 2048 or 4096, you must

also enable jumbo frames on all switches in the network path for all peer hosts. For more information about the RoCE maximum transmission unit, see z/OS Communications Server: IP Configuration Guide.

FIXEDMEMORY *mem_size*
Specifies the maximum amount of 64-bit storage that the stack can use for the send and receive buffers that are required for SMC-R communications. The *mem_size* value is an integer in the range 30 - 9999, and represents the maximum storage in megabytes of data. The default value is 256 megabytes.

TCPKEEPMININTERVAL *interval*
This interval specifies the minimum interval that TCP keepalive packets are sent on the TCP path of an SMC-R link.

Rules:

- If a keepalive interval is also specified on the INTERVAL parameter of the TCPCONFIG statement or is set for a specific SMC-R link socket by the TCP_KEEPALIVE setsockopt() option, the largest of the three interval values is used.
- The valid range for this interval is 0-2147460 seconds, and the default is 300 seconds.
- A value of 0 disables TCP keepalive probe packets on the TCP path of an SMC-R link.
- The SO_KEEPALIVE setsockopt() option must be set for keepalive processing to be used.

Result: The TCPKEEPMININTERVAL setting has no effect on keepalive processing for the SMC-R path of an SMC-R link.

For more information about TCP keepalive processing for the TCP path and the SMC-R path of SMC-R links, see TCP keepalive in z/OS Communications Server: IP Configuration Guide.

SYSPLEXMONITOR
Specifies SYSPLEXMONITOR subparameters to configure the operation of the sysplex autonomics function. For more information about connectivity problems in a sysplex, see z/OS Communications Server: IP Configuration Guide.

If the SYSPLEXMONITOR parameter is not specified in the initial TCP/IP profile, then the sysplex autonomics function uses the default values for all SYSPLEXMONITOR subparameters. If the SYSPLEXMONITOR parameter is specified but not all subparameters are specified in the initial TCP/IP profile, then the sysplex autonomics function uses the default values for those SYSPLEXMONITOR subparameters that are not specified. For example, if SYSPLEXMONITOR is specified without RECOVERY or NORECOVERY specified in the initial profile, then the NORECOVERY action is in effect.

Rule: If you specify the GLOBALCONFIG statement in a data set associated with a VARY TCPIP,,OBEYFILE command and the SYSPLEXMONITOR parameter is specified without any subparameters, an informational message is issued and the parameter is ignored.

AUTOREJOIN | NOAUTOREJOIN

Specifies whether TCP/IP should automatically rejoin the TCP/IP sysplex group when a detected problem is relieved after the stack has left the sysplex group.

NOAUTOREJOIN

Do not rejoin the TCP/IP sysplex group when a detected problem is relieved. This is the default value.

AUTOREJOIN

When all detected problems (that caused the stack to leave the sysplex group) are relieved, the stack automatically rejoins the sysplex group and reprocesses the saved VIPADYNAMIC block configuration.

Restriction: AUTOREJOIN cannot be configured when NORECOVERY is configured (or set to the default value).

Guideline: AUTOREJOIN should be used when RECOVERY is configured to allow the stack to rejoin the sysplex group without operator intervention.

DELAYJOIN | NODELAYJOIN

Specify whether TCP/IP should delay joining or rejoining the TCP/IP sysplex group (EZBTCPCS) during stack initialization, or rejoining the sysplex group following a VARY TCPIP,,OBEYFILE command.

NODELAYJOIN

Attempt to join the TCP/IP sysplex group. When specified during stack initialization, the stack attempts to join the sysplex group. This is the default value.

DELAYJOIN

Delay joining the TCP/IP sysplex group and processing any VIPADYNAMIC block or DYNAMICXCF statements during stack initialization until OMPROUTE is started and active.

DYNROUTE | NODYNROUTE

Specifies whether TCP/IP should monitor the presence of dynamic routes over monitored network links or interfaces.

NODYNROUTE

The TCP/IP stack should not monitor the presence of dynamic routes over monitored network links or interfaces. When MONINTERFACE is not configured, this is the default value.

DYNROUTE

The TCP/IP stack should monitor the presence of dynamic routes over monitored network links or interfaces.

Tip: This level of monitoring is useful in detecting problems that OMPROUTE is having in communicating with other routing daemons on the selected network interfaces.

If no dynamic routes are present in the TCP/IP stack from that network, a specific interface attached to that network might not be active or routers attached to that network might not be active or healthy. In either case, when these conditions are detected, they provide a reasonable indication that client requests for DVIPAs or distributed DVIPAs owned by this TCP/IP stack might not reach this stack over that interface. These checks can help further qualify the state of a network

interface on this TCP/IP stack. When the MONINTERFACE parameter is specified, This is the default value.

Restriction: DYNROUTE cannot be specified when NOMONINTERFACE is configured (or is the default value).

Rules:

- Specify DYNROUTE only when OMPROUTE is configured and started; otherwise, the TCP/IP stack might be forced to leave the TCP/IP sysplex group if RECOVERY is coded.
- If DYNROUTE is specified, also specify DELAYJOIN to avoid a scenario where the TCP/IP stack leaves the TCP/IP sysplex group before OMPROUTE is started.

NOJOIN

Specifies that the TCP/IP stack should not join the TCP/IP sysplex group (EZBTCPCS) during stack initialization. If this value is specified, the TCP/IP stack does not process any VIPADYNAMIC block or DYNAMICXCF statements. Any other GLOBALCONFIG SYSPLEXMONITOR parameter settings (configured or default) are ignored, and the settings are saved in case you want the TCP/IP stack to join the sysplex group at a later time.

If you subsequently issue a VARY TCPIP,,SYSPLEX,JOINGROUP command, the NOJOIN setting is overridden and the saved GLOBALCONFIG SYSPLEXMONITOR parameter settings become active. For example, if you configure NOJOIN and DELAYJOIN, DELAYJOIN is initially ignored. If you subsequently issue a V TCPIP,,SYSPLEX,JOINGROUP command, NOJOIN is overridden, DELAYJOIN becomes active, and the stack joins the sysplex group if OMPROUTE is initialized.

Any sysplex-related definitions within the TCP/IP profile, such as VIPADYNAMIC or IPCONFIG DYNAMICXCF statements, are not processed until the TCP/IP stack joins the sysplex group.

Restriction: You can specify this parameter only in the initial profile; you cannot specify it when you issue a VARY TCPIP,,OBEYFILE command.

MONINTERFACE | NOMONINTERFACE

NOMONINTERFACE

The TCP/IP stack should not monitor the status of any network links or interfaces. This is the default.

MONINTERFACE

The TCP/IP stack should monitor the status of specified network link or interfaces. The interfaces or links being monitored are those that are configured with the MONSYSPLEX keyword on the LINK or INTERFACE statement. See Summary of DEVICE and LINK statements or Summary of INTERFACE statements for more information.

Guideline: This level of monitoring can further qualify the health of the TCP/IP stack by ensuring that at least one key interface is active and available. This option can be useful in environments where the dynamic XCF interface is not configured as an alternate network path

for this stack (for example, where no dynamic routes are advertised over dynamic XCF interfaces and no static or replaceable static routes are defined over those interfaces).

RECOVERY | NORECOVERY
Specify the action to be taken when a sysplex problem is detected.

NORECOVERY
When a problem is detected, issue messages regarding the problem but take no further action. This is the default value.

RECOVERY
When a problem is detected, issue messages regarding the problem, leave the TCP/IP sysplex group, and delete all DVIPA resources owned by this stack. As allowed by a configuration with backup capabilities, other members of the TCP/IP sysplex automatically take over the functions of this member that was removed from the TCP/IP sysplex group.

Recovery is the preferred method of operation because other members of the TCP/IP sysplex can automatically take over the functions of a member with no actions needed by an operator. IBM Health Checker for z/OS enhancements can be used to check whether the RECOVERY parameter has been specified when the IPCONFIG DYNAMICXCF or IPCONFIG6 DYNAMICXCF parameters have been specified. For more details about IBM Health Checker for z/OS enhancements, see the IBM Health Checker for z/OS enhancements information in the z/OS Communications Server: IP Diagnosis Guide.

TIMERSECS *seconds*
Time value specified in seconds. Determines how quickly the sysplex monitor reacts to problems with needed sysplex resources. Valid values are in the range 10 - 3600 seconds. The default value is 60 seconds.

SYSPLEXWLMPOLL *seconds*
Time value specified in seconds. Determines how quickly the sysplex distributor and its target servers poll WLM for new weight values. A short time results in quicker reactions to changes in target status. Valid values are in the range is 1 - 180 seconds. The default value is 60 seconds.

TCPIPSTATISTICS | NOTCPIPSTATISTICS

NOTCPIPSTATISTICS
Indicates that the TCP/IP counter values are not to be written to the output data set designated by the CFGPRINT JCL statement.

The NOTCPIPSTATISTICS parameter is confirmed by the message:

```
EZZ0613I TCPIPSTATISTICS IS DISABLED
```

This is the default value.

TCPIPSTATISTICS
Prints the values of several TCP/IP counters to the output data set designated by the CFGPRINT JCL statement. These counters include number of TCP retransmissions and the total number of TCP segments sent from the MVS™ TCP/IP system. These TCP/IP statistics are written to the designated output data set only during termination of the TCP/IP address space.

The TCPIPSTATISTICS parameter is confirmed by the message:

```
EZZ0613I TCPIPSTATISTICS IS ENABLED
```

The SMFCONFIG TCPIPSTATISTICS parameter (see SMFCONFIG statement) serves a different purpose. It requests that SMF records of subtype 5 containing TCP/IP statistics be created. These statistics are recorded in SMF type 118 or 119, subtype 5 records.

WLMPRIORITYQ | NOWLMPRIORITYQ

Specifies whether OSA-Express QDIO write priority values should be assigned to packets associated with WorkLoad Manager service classes, and to forwarded packets. See the information about prioritizing outbound OSA-Express data using the WorkLoad Manager service class in z/OS Communications Server: IP Configuration Guide .

NOWLMPRIORITYQ

Specifies that OSA-Express QDIO write priority values should not be assigned to packets associated with WorkLoad Manager service class values or to forwarded packets. This value is the default.

WLMPRIORITYQ

Specifies that OSA-Express QDIO write priority values should be assigned to packets associated with WorkLoad Manager service class valuesand to forwarded packets.

You can assign specific OSA-Express QDIO write priority values by using the IOPRI*n* subparameters, where *n* is one or more of the priority values in the range 1 - 4. For each subparameter, you can specify a control value in the range 0 - 6, which correlates to the WLM services classes, or you can specify the keyword FWD for forwarded packets. WLM supports a service class for the SYSTEM value, but this value is always assigned the OSA-Express QDIO write priority 1 and its assignment cannot be configured; therefore, a control value is not assigned for the SYSTEM WLM service class.

You can use the default assignment by specifying the WLMPRIORITYQ parameter without any IOPRI*n* subparameters. See the description of the *default_control_values* variable in this topic to understand the default assignment.

control_values

Control values are used to represent the WLM service classes and forwarded packets. Valid control values are the digits 0 - 6, which represent WLM service classes, or the keyword FWD, which represents forwarded packets. Table 4 identifies the control value, the type of packet that it represents, and the default QDIO priority assigned to the packet:

Table 4. WLM Service Class Importance Levels

Control value	Type of packet	Default QDIO priority
0	System-defined service class (SYSSTC) used for high-priority started tasks	1
1	User-defined service classes with importance level 1	2
2	User-defined service classes with importance level 2	3
3	User-defined service classes with importance level 3	3

Table 4. WLM Service Class Importance Levels (continued)

Control value	Type of packet	Default QDIO priority
4	User-defined service classes with importance level 4	4
5	User-defined service classes with importance level 5	4
6	User-defined service classes associated with a discretionary goal	4
FWD	Forwarded packets	4

default_control_values
When the WLMPRIORITYQ parameter is specified without any IOPRIn subparameters, then the OSA-Express QDIO write priority values are assigned as shown Table 4 on page 71.

IOPRI*n control_values*
Use the IOPRIn subparameters to correlate control values with specific OSA-Express QDIO write priority values. You can use one or more of the following subparameter keywords:

- IOPRI1
- IOPRI2
- IOPRI3
- IOPRI4

Each subparameter keyword corresponds to one of the four QDIO write priority values, 1 through 4. Each subparameter can be specified once on a GLOBALCONFIG statement.

control_values
Indicates the type of packet to which the QDIO write priority value should be assigned. Valid values are:

Digits 0 - 6
Causes the QDIO write priority value that is specified by the IOPRI*n* subparameter to be assigned to packets associated with the WLM service classes represented by the control value.

FWD This keyword causes the QDIO write priority value indicated by the IOPRIn subparameter to be assigned to forwarded packets.

Rules:

- IOPRIn must be followed by one or more priority level releases.
- You can specify more than one control value for an IOPRIn subparameter. Each control value must be separated by at least one blank.
- A specific control value can be specified only once in the set of IOPRIn subparameters on a GLOBALCONFIG statement.
- If any control value is not explicitly specified on an IOPRI*n* subparameter, then the associated packets are assigned a default QDIO write priority 4.

In the following example, QDIO priority 1 is assigned to packets associated with control values 0 and 1, QDIO priority 2 is assigned to packets associated with control value 2 and to forwarded packets, QDIO priority 3 is assigned to packets associated with control values 3 and 4, and QDIO priority 4 is assigned to packets associated with control values 5 and 6.

```
WLMPRIORITYQ  IOPRI1 0 1
              IOPRI2 2 FWD
              IOPRI3 3 4
              IOPRI4 5 6
```

XCFGRPID *group_id*

This parameter is needed only if you want subplexing. If specified, the value provides a 2-digit suffix that is used in generating the XCF group name that the TCP/IP stack joins. Valid values are in the range 2 - 31. The group name is EZBT*vvtt*, where the *vv* value is the VTAM XCF group ID suffix (specified with the XCFGRPID VTAM start option) and the *tt* value is the *group_id* value supplied on this parameter, used as a 2-digit value converted to character format. If no VTAM XCF group ID suffix was specified, the group name is EZBTCP*tt.* If no VTAM XCF group ID suffix and no TCP XCF group ID suffix is specified, the group name is EZBTCPCS.

These characters are also used as a suffix for the EZBDVIPA and EZBEPORT structure names, in the form EZBDVIPA*vvtt* and EZBEPORT*vvtt*. If no VTAM XCF group ID suffix was specified, the structure names are EZBDVIPA01*tt* and EZBEPORT01*tt*.

If XCFGRPID is not specified, the XCF group name is EZBTvvCS and the structure names are EZBDVIPA*vv* and EZBEPORT*vv*. If no VTAM XCF group id suffix was specified, the group name is EZBTCPCS and the structure names are EZBDVIPA and EZBEPORT.

Restriction: XCFGRPID can be specified only in the initial profile.

This allows multiple TCP/IP stacks to join separate Sysplex groups and access separate Coupling Facility structures, isolating sets of TCP/IP stacks into subplexes with XCF communication only with other TCP/IP stacks within the same subplex.

If HiperSockets is supported on this system, the IQDVLANID parameter, on the GLOBALCONFIG statement, must be specified if XCFGRPID is specified. Stacks on the same CPC using the same HiperSockets CHPID that specify the same XCFGRPID value must specify the same IQDVLANID value.

Stacks on the same CPC using the same HiperSockets CHPID specifying different XCFGRPID values must specify different IQDVLANID values. This allows partitioning of connectivity across the Sysplex to include partitioning of connectivity across HiperSockets.

Creating TCP/IP and VTAM subplexes can add some complexity to your VTAM and TCP/IP configurations and requires careful planning. Before setting this parameter you should review the information about setting up a subplex in the z/OS Communications Server: IP Configuration Guide.

ZIIP

Specifies subparameters that control whether TCP/IP displaces CPU cycles onto a System z9® Integrated Information Processor (zIIP). You must specify at least one subparameter. If the ZIIP parameter is specified with no subparameters, an informational message is issued and the parameter is ignored.

IPSECURITY | NOIPSECURITY
Specifies whether TCP/IP should displace CPU cycles for IPSec workload to a zIIP. For more information about this function, see the Additional IPSec assist using z9® Integrated Information Processor (zIIP IP security) topic in z/OS Communications Server: IP Configuration Guide.

NOIPSECURITY
Do not displace CPU cycles for IPSec workload to a zIIP. This is the default value.

IPSECURITY
When possible, displace CPU cycles for IPSec workload to a zIIP. Workload Manager (WLM) definitions should be examined and possible changes made before this option is used. See the more detailed description in the additional IPSec Assist by way of z9 Integrated Information Processor (zIIP IPSECURITY) topic in z/OS Communications Server: IP Configuration Guide.

IQDIOMULTIWRITE | NOIQDIOMULTIWRITE
Specifies whether TCP/IP should displace CPU cycles for large outbound TCP messages that are typically created by traditional streaming work loads such as file transfer, and interactive web-based service workloads such as XML or SOAP. The TCP/IP outbound message must be at least 32KB in length before the write processing is off-loaded to an available zIIP specialty engine. For more information about this function, see the information about HiperSockets multiple write assist with IBM zIIP in z/OS Communications Server: IP Configuration Guide.

NOIQDIOMULTIWRITE
Do not displace CPU cycles for the writing of large TCP outbound messages to a zIIP. This is the default value.

IQDIOMULTIWRITE
When possible, displace CPU cycles for the writing of large TCP outbound messages to a zIIP.

Rules:

- You cannot specify IQDIOMULTIWRITE as a ZIIP parameter when GLOBALCONFIG IQDMULTIWRITE is not configured. When GLOBALCONFIG IQDMULTIWRITE is not configured, HiperSockets interfaces do not use the multiple write support.
- Only large TCP outbound messages (32KB and larger) are processed on the zIIP specialty engine.
- The TCP message must be originating from this node. Routed TCP messages are not eligible for zIIP assistance.

Tip: These ZIIP parameters apply to pre-defined HiperSockets interfaces, as well as HiperSockets interfaces that are created and used by dynamic XCF definitions.

Steps for modifying

To modify parameters for the GLOBALCONFIG statement, you must respecify the statement with the new parameters.

The following list describes how to modify individual parameters:

AUTOIQDX and NOAUTOIQDX
If you use the VARY TCPIP,,OBEYFILE command to change this parameter

from AUTOIQDX to NOAUTOIQDX, no new dynamic IQDX interfaces will be activated. All active dynamic IQDX interfaces will remain active and available for use. To stop existing interfaces, you must issue a V TCPIP,,STOP command for each active IQDX interface.

If you use the VARY TCPIP,,OBEYFILE command to change this parameter from NOAUTOIQDX to AUTOIQDX, active OSX interfaces are not affected, but the stack will attempt to activate a dynamic IQDX interface on any subsequent OSX activations.

EXPLICITBINDPORTRANGE and NOEXPLICITBINDPORTRANGE

If you specified the EXPLICITBINDPORTRANGE parameter and then you change to the NOEXPLICITBINDRANGE parameter, then the stack stops allocating more ports from the EXPLICITBINDPORTRANGE pool. However, the existing active range for the EXPLICITBINDPORTRANGE pool in the coupling facility is unaffected unless you are changing the parameter on the last stack in the sysplex using this function.

If you specified the NOEXPLICITBINDPORTRANGE parameter and then you change to the EXPLICITBINDPORTRANGE parameter, then a range of ports used for the EXPLICITBINDPORTRANGE pool is set. The stack uses ports from that pool for explicit bind() requests to the IPv4 INADDR_ANY address, or to the IPv6 unspecified address (in6addr_any), and port 0. If the range specified on the EXPLICITBINDPORTRANGE parameter is different from the currently active range for the EXPLICITBINDPORTRANGE pool in the coupling facility, the new range replaces that value.

Changing the starting port (*1st_port*), the number of ports (*num_ports*), or both for the EXPLICITBINDPORTRANGE parameter changes the port numbers in the pool of ports that is guaranteed to be unique across the sysplex for future port allocation

Guidelines:

- Changing the range specified on the EXPLICITBINDPORTRANGE parameter of the GLOBALCONFIG statement affects every stack in the sysplex that has configured a GLOBALCONFIG EXPLICITBINDPORTRANGE value. Future port allocations for all such stacks use the new port range.
- Ports in the EXPLICITBINDPORTRANGE range are usually assigned to a stack in blocks of 64 ports. When expanding the range, use multiples of 64 multiplied by the number of stacks that use a GLOBALCONFIG EXPLICITBINDPORTRANGE configuration.

IQDMULTIWRITE and NOIQDMULTIWRITE

If this parameter is changed with the VARY TCPIP,,OBEYFILE command, the new value does not take effect for any active HiperSockets (iQDIO) interfaces. For a change in this parameter to take effect for an active iQDIO interface, you must stop and restart both the IPv4 and IPv6 interface for the change to be effective.

IQDVLANID

If the IQDVLANID parameter was previously specified and you modify that value, then you must stop and restart the TCP/IP stack for the change to take effect.

MLSCHKTERMINATE

You cannot change the MLSCHKTERMINATE parameter to the NOMLSCHKTERMINATE parameter when the RACF® option MLSTABLE

is on and the RACF option MLQUIET is off. You can always change the NOMLSCHKTERMINATE parameter to the MLSCHKTERMINATE parameter, but this change is ignored if the value is specified in the data set of a VARY TCPIP,,OBEYFILE command and consistency errors are detected at the same time.

SEGMENTATIONOFFLOAD and NOSEGMENTATIONOFFLOAD

If this parameter is changed with the VARY TCPIP,,OBEYFILE command, the new value does not take effect for any active OSA-Express QDIO interfaces. For a change in these parameters to take effect, all the OSA-Express QDIO interfaces that support TCP segmentation offload must be stopped and restarted.

SMCD and NOSMCD

- If SMC-D support is not enabled, you can specify the SMCD parameter in a VARY TCPIP,,OBEYFILE command data set to activate the support.

  Result: TCP/IP retains knowledge of the last set of SMCD subparameter values that are specified on the GLOBALCONFIG statement, even if GLOBALCONFIG NOSMCD was specified subsequently. If you issue a VARY TCPIP,,OBEYFILE command with GLOBALCONFIG SMCD specified, TCP/IP uses the last saved set of SMCD subparameters, unless new values for the subparameters are coded on the GLOBALCONFIG SMCD statement. Therefore, you can temporarily stop SMC-D processing by issuing a VARY TCPIP,,OBEYFILE command with GLOBALCONFIG NOSMCD specified. Then you can resume SMC-D processing with the previous subparameter settings by issuing a second VARY TCPIP,,OBEYFILE command with just GLOBALCONFIG SMCD specified. Specifying the SMCD parameter also causes the AUTOCACHE function and AUTOSMC monitoring function to be restarted if the SMCGLOBAL AUTOCACHE and AUTOSMC parameters are enabled.
- If SMC-D support is enabled, you can specify the NOSMCD parameter in a VARY TCPIP,,OBEYFILE command data set to deactivate the support.
  - No new TCP connections that use SMC-D processing will be established.
  - Existing TCP connections that use SMC-D will continue to use SMC-D processing.
  - The AUTOCACHE function will be stopped if SMC-R processing is not active.
  - The AUTOSMC monitoring function will be stopped if SMC-R processing is not active.

SMCGLOBAL

AUTOCACHE and NOAUTOCACHE

If you use the VARY TCPIP,,OBEYFILE command to change this parameter from AUTOCACHE to NOAUTOCACHE, the following actions occur:

- Destination IP addresses cached not to use SMC will be deleted from the cache.
- The stack will not cache unsuccessful attempts to create an SMC-R or SMC-D link per destination IP address for new TCP connections.

If you use the VARY TCPIP,,OBEYFILE command to change this parameter from NOAUTOCACHE to AUTOCACHE, the SMCGLOBAL AUTOCACHE function is enabled.

SMCR and NOSMCR

- If SMCR support is not enabled, you can specify the SMCR parameter in a VARY TCPIP,,OBEYFILE command data set to activate the support.

  Result: TCP/IP retains knowledge of the last set of SMCR subparameter values that are specified on the GLOBALCONFIG statement, even if GLOBALCONFIG NOSMCR was specified subsequently. If you issue a VARY TCPIP,,OBEYFILE command with GLOBALCONFIG SMCR specified, TCP/IP uses the saved last set of SMCR subparameters, unless new values for the subparameters are coded on the GLOBALCONFIG SMCR statement. This allows you to temporarily stop SMC-R processing by issuing a VARY TCPIP,,OBEYFILE command with GLOBALCONFIG NOSMCR specified. Then you can resume SMC-R processing with the previous subparameter settings by issuing a second VARY TCPIP,,OBEYFILE command with just GLOBALCONFIG SMCR specified.Specifying the SMCR parameter also causes the AUTOCACHE function and AUTOSMC monitoring function to be restarted if the SMCGLOBAL AUTOCACHE and AUTOSMC parameters are enabled.
- If SMCR support is enabled, you can specify the NOSMCR parameter in a VARY TCPIP,,OBEYFILE command data set to deactivate the support.
  - No new TCP connections that use SMC-R processing will be established.
  - Existing TCP connections that use SMC-R will continue to use SMC-R processing.
  - The AUTOCACHE function will be stopped if SMC-D processing is not active.
  - The AUTOSMC monitoring function will be stopped if SMC-D processing is not active.
- You cannot change the SMCR PFID parameter values that are currently configured when the associated 10GbE RoCE Express interfaces are active. To change the SMCR PFID parameter values that are currently configured, you must perform the following steps in order:
  1. Stop the associated 10GbE RoCE Express interfaces.
  2. Issue the VARY TCPIP,,OBEYFILE command with the new PFID values that are coded in the command data set. The new PFID values replace the existing PFID values.
- To add PFID values when you have one or more PFID values coded, you must specify the existing PFID values and the additional PFID values on the SMCR parameter in the VARY TCPIP,,OBEYFILE command data set. Existing PFID values and any existing 10GbE RoCE Express interfaces are not affected.

SYSPLEXMONITOR

AUTOREJOIN and NOAUTOREJOIN

If you change NOAUTOREJOIN to AUTOREJOIN after the stack has left the sysplex and before the problem that caused it to leave has been relieved, the stack automatically rejoins the sysplex group when the problem is relieved. However, if you change NOAUTOREJOIN to AUTOREJOIN after the problem that caused

the stack to leave the group has been relieved, you must issue a VARY TCPIP,,SYSPLEX,JOINGROUP command to cause the stack to rejoin the sysplex.

DELAYJOIN and NODELAYJOIN
Changing from DELAYJOIN to NODELAYJOIN while the TCP/IP stack is in the process of delaying joining the sysplex group because OMPROUTE is not active causes the TCP/IP stack to immediately join the sysplex group.

Changing from NODELAYJOIN to DELAYJOIN has no immediate effect until the TCP/IP stack leaves the sysplex group and then attempts to rejoin while OMPROUTE is not active.

SYSPLEXWLMPOLL
You can change the polling rate for WLM values while the TCP/IP stack is active. In order for the change to be effective, you should change the polling rate on all stacks that participate in sysplex distribution (all active distributing stacks, any backup stacks that might take over distribution, and all target stacks).

WLMPRIORITYQ
If you specify WLMPRIORITYQ with the VARY TCPIP,,OBEYFILE command, the IOPRI*n* values are changed to the values specified for the *default_control_values* variable. The new values take effect immediately for all workloads influenced by this function.

WLMPRIORITYQ IOPRIn *control_values*
If you specify this parameter with the VARY TCPIP,,OBEYFILE command, and you do not specify all the control values, the QDIO priority 4 is assigned to packets associated with all control values omitted. The new values immediately take effect for all workloads influenced by this function.

Rule: You cannot modify individual IOPRI*n* control values. If you attempt to modify IOPRI*n* control values, but you specify only those control values that you want to modify, then the QDIO priority 4 is assigned to packets that are associated with any control values that you omitted.

XCFGRPID
For a change in this parameter to take effect, you must stop and restart the TCP/IP stack.

Examples

This example shows the use of the SYSPLEXMONITOR parameter on the GLOBALCONFIG statement that enables many of the sysplex autonomics functions:

```
GLOBALCONFIG SYSPLEXMONITOR AUTOREJOIN DELAYJOIN MONINTERFACE DYNROUTE RECOVERY
```

The following example shows the use of the EXPLICITBINDPORTRANGE parameter to define 1024 ports in the range 5000 - 6023. The ports are used for explicit binds to the IPv4 INADDR_ANY address, or to the IPv6 unspecified address (in6addr_any), and port 0:

```
GLOBALCONFIG EXPLICITBINDPORTRANGE 5000 1024
```

The following example shows the use of the SMCR parameter to define two 10GbE RoCE Express features that use PFID values 0018 and 0019 and port numbers 1 and 2, and to limit the stack to 500 megabytes of 64-bit storage for SMC-R communications.

```
GLOBALCONFIG SMCR PFID 0018 PORTNUM 1 PFID 0019 PORTNUM 2 FIXEDMEMORY 500
```

The following example shows the use of the SMCD parameter to enable SMC-D support and limit the stack to 500 megabytes of 64-bit storage for SMC-D communications.

```
GLOBALCONFIG SMCD FIXEDMEMORY 500
```

Related topics

- SMFCONFIG statement
- For more information about TCP/IP networking in a multilevel-secure environment, see the security information in z/OS Communications Server: IP Configuration Guide.

INTERFACE - IPAQENET OSA-Express QDIO interfaces statement

Use the INTERFACE statement to specify an OSA-Express QDIO Ethernet interface for IPv4.

Restriction: This statement applies to IPv4 IP addresses only.

To determine the OSA-Express microcode level, use the DISPLAY TRL command. If a specific OSA-Express function is documented with a minimum microcode level, you can use this command to determine whether that function is supported. IBM service might request the microcode level for problem diagnosis. For more information about the DISPLAY TRL command, see z/OS Communications Server: SNA Operation.

The following OSA-Express features can be defined in QDIO mode for IPv4:

- Fast Ethernet
- Gigabit Ethernet
- 1000BASE-T Ethernet
- 10G Ethernet

When you start an IPAQENET interface (and you did not specify VMAC with ROUTEALL), TCP/IP registers all non-loopback local (home) IPv4 addresses for this TCP/IP instance to the OSA-Express feature. If you subsequently add, delete, or change any home IPv4 addresses on this TCP/IP instance, TCP/IP dynamically registers the changes to the OSA-Express feature. The OSA adapter routes datagrams destined for those IPv4 addresses to this TCP/IP instance.

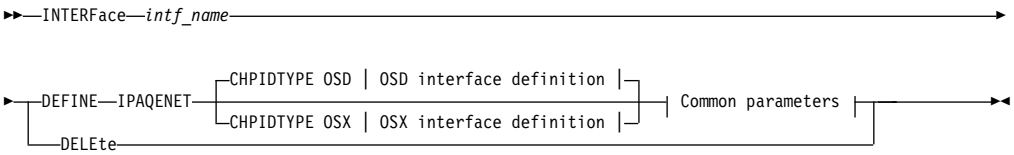
If a datagram is received at the OSA adapter for an unregistered IPv4 address, then the OSA-Express feature routes the datagram to the TCP/IP instance, depending on the setting of a virtual MAC (VMAC) address or definition of an instance as PRIROUTER or SECROUTER. If the datagram is not destined for a virtual MAC address and no active TCP/IP instance using this interface is defined as PRIROUTER or SECROUTER, then the OSA-Express feature discards the datagram. See the router information in z/OS Communications Server: IP Configuration Guide for more details and primary and secondary routing in z/OS Communications Server: SNA Network Implementation Guide.

For detailed instructions on setting up an OSA-Express feature, see zEnterprise System and System z10 OSA-Express Customer's Guide and Reference.

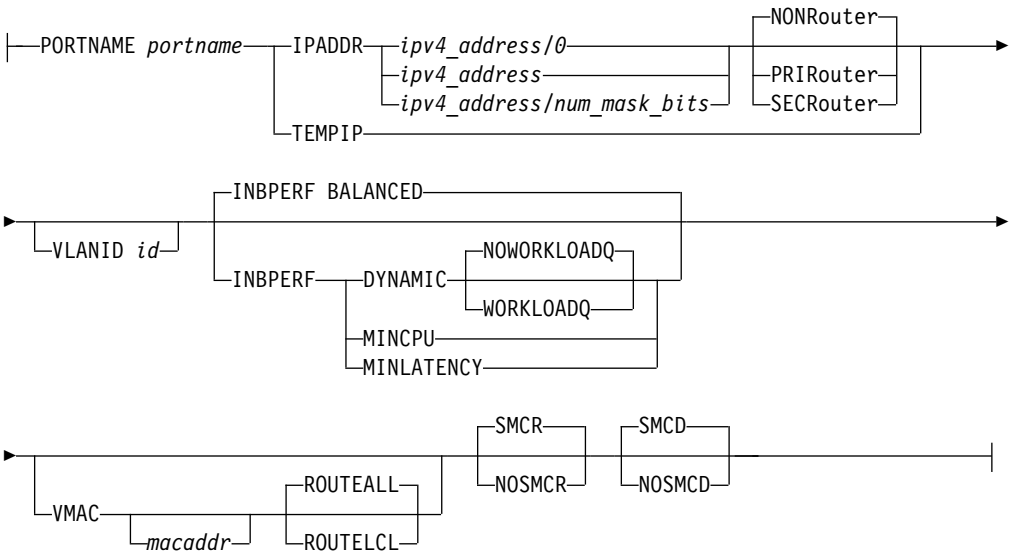
For more information about missing interrupt handler (MIH) considerations with TCP/IP interfaces, see Missing interrupt handler factors.

Syntax

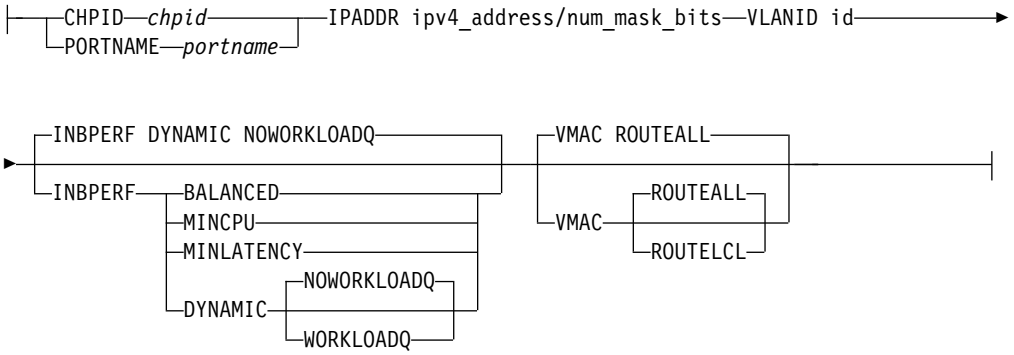
Rule: Specify the required parameters and the CHPIDTYPE parameter in the order shown here. The OSD Interface Definition and OSX Interface Definition parameters can be specified in any order.



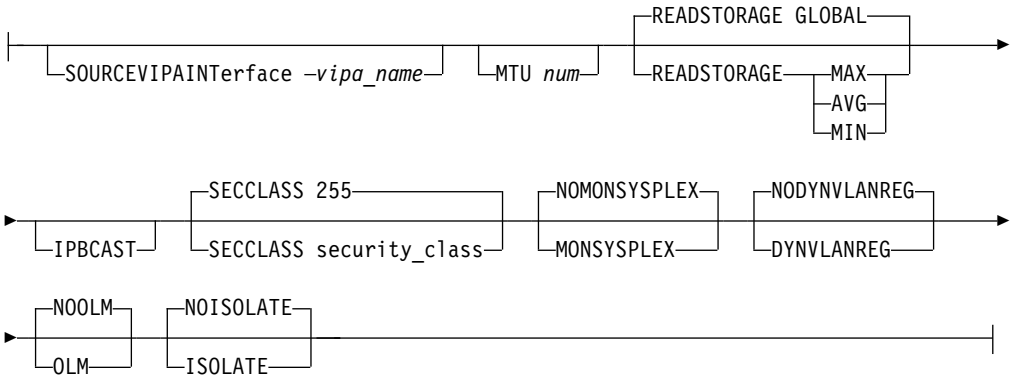
OSD Interface Definition:



OSX Interface Definition:



Common parameters for OSD and OSX interface definitions:



Parameters

intf_name
The name of the interface. The maximum length is 16 characters.

Requirement: This name must be different than the name specified for the PORTNAME parameter.

DEFINE
Specifies that this definition is to be added to the list of defined interfaces.

DELETE
Specifies that this definition is to be deleted from the list of defined interfaces. The *intf_name* value must be the name of an interface previously defined by an INTERFACE statement. Specifying INTERFACE DELETE deletes the home IP address for the interface.

IPAQENET
Indicates that the interface uses the interface based on IP assist, which belongs to the QDIO family of interfaces, and uses the Ethernet protocol.

CHPIDTYPE
An optional parameter indicating the CHPID type of the OSA-Express QDIO interface.

OSD Indicates an external data network type. This is the default value.

OSX The intraensemble data network. See z/OS Communications Server: IP Configuration Guide for information about requirements necessary to make an OSX work.

Rule: You must specify an OSD interface definition to make this interface eligible to use Shared Memory Communications over Remote Direct Memory Access (SMC-R) or Shared Memory Communications - Direct Memory Access (SMC-D).

CHPID *chpid*
This parameter applies only to interfaces of CHPIDTYPE OSX and is used to specify the CHPID for the interface. This value is a 2-character hexadecimal value (00 - FF).

PORTNAME *portname*
Use this parameter to specify the PORT name that is in the TRLE definition for

the QDIO interface. The TRLE must be defined as MPCLEVEL=QDIO. For details about defining a TRLE, see z/OS Communications Server: SNA Resource Definition Reference.

Requirement: The *portname* value must be different than the name specified for *intf_name*.

IPADDR

ipv4_address
The home IP address for this interface.

Requirement: The IP address must be specified in dotted decimal form.

num_mask_bits
An integer value in the range 0 - 32 that represents the number of leftmost significant bits for the subnet mask of the interface. This value also controls how ARP processing for VIPAs is handled for this interface. When you specify a nonzero value, the TCP/IP stack informs OSA to perform ARP processing for a VIPA only if the VIPA is configured in the same subnet as the OSA (as defined by this subnet mask). The default is 0 for CHPIDTYPE OSD. This parameter is required for CHPIDTYPE OSX..

Requirement: If you are configuring multiple IPv4 VLAN interfaces to the same OSA-Express feature, then you must specify a nonzero value for the *num_mask_bits* variable for each of these interfaces and the resulting subnet must be unique for each of these interfaces.

Rule: If you are using OMPROUTE and OMPROUTE is not configured to ignore this interface, ensure that the subnet mask value that you define on this parameter matches the subnet mask used by OMPROUTE for this interface. The subnet mask used by OMPROUTE is the subnet mask value defined on the corresponding OMPROUTE statement (OSPF_INTERFACE, RIP_INTERFACE, or INTERFACE) for this interface. If no OMPROUTE statement is specified for this interface, the subnet mask used by OMPROUTE is the class mask for the interface IP address.

TEMPIP
Specifies that the interface starts with an IP address of 0.0.0.0. The interface can be used for broadcast traffic. This parameter applies only to interfaces that are defined with CHPIDTYPE OSD.

Guideline: Use TEMPIP interfaces in a unit test environment to support an application that provides a DHCP client, such as IBM Rational® Developer for System z Unit Test feature (Rdz-UT). For more information about configuring a TEMPIP interface, see Using TEMPIP interfaces in z/OS Communications Server: IP Configuration Guide.

NONROUTER
If a datagram is received at this interface for an unknown IP address, the datagram is not routed to this TCP/IP instance. This is the default value.

The PRIROUTER and SECROUTER parameters interact with the VLANID parameter. See the VLANID parameter definition to understand this relationship.

For more information about VLANID parameter interactions, see z/OS Communications Server: IP Configuration Guide.

Rule: This keyword applies only to interfaces of CHPIDTYPE OSD and is ignored if the VMAC parameter is configured on the INTERFACE statement.

PRIROUTER

If a datagram is received at this interface for an unknown IP address and is not destined for a virtual MAC, the datagram is routed to this TCP/IP instance. This parameter interacts with the VLANID parameter. See the VLANID parameter definition to understand this relationship.

For more information about VLANID parameter interactions, see z/OS Communications Server: IP Configuration Guide.

Rule: This keyword applies only to interfaces of CHPIDTYPE OSD and is ignored if the VMAC parameter is configured on the INTERFACE statement.

SECROUTER

If a datagram is received at this interface for an unknown IP address and is not destined for a virtual MAC, and there is no active TCP/IP instance defined as PRIROUTER, then the datagram is routed to this TCP/IP instance. This parameter interacts with the VLANID parameter. See the VLANID parameter definition to understand this relationship.

For more information about VLANID parameter interactions, see z/OS Communications Server: IP Configuration Guide.

Rule: This keyword applies only to interfaces of CHPIDTYPE OSD and is ignored if the VMAC parameter is configured on the INTERFACE statement.

VLANID id

Specifies the decimal virtual LAN identifier to be assigned to the OSA-Express interface. This field should be a virtual LAN identifier recognized by the switch for the LAN that is connected to this OSA-Express interface. The valid range is 1 - 4094. This parameter is optional for CHPIDTYPE OSD and required for CHPIDTYPE OSX.

Guideline: Installation configuration on other platforms or related to Ensemble networking can limit the maximum VLANID of 4096.

The VLANID parameter interacts with the PRIROUTER and SECROUTER parameters. If you configure both the VLANID parameter and either PRIROUTER or SECROUTER parameter, then this TCP/IP instance acts as a router for this VLAN (ID) only. Datagrams that are received at this device instance for an unknown IP address and are not destined for a virtual MAC are routed only to this TCP/IP instance if it is VLAN tagged with this VLAN ID. For more information about VLANID parameter interactions, see z/OS Communications Server: IP Configuration Guide.

Rule: If you are configuring multiple VLAN interfaces to the same OSA-Express feature, then you must specify the VMAC parameter (with the default ROUTEALL attribute) on the INTERFACE statement for each of these interfaces.

Restriction: The stack supports a maximum of 32 IPv4 VLAN interfaces to the same OSA-Express port. Additional VLANID limitations might exist if this interface can be used with Shared Memory Communications over Remote Direct Memory Access (SMC-R). See VLANID considerations in z/OS Communications Server: IP Configuration Guide for details.

INBPERF

An optional parameter that indicates how processing of inbound traffic for the QDIO interface is performed.

There are three supported static settings that indicate how frequently the adapter should interrupt the host for inbound traffic: BALANCED, MINCPU, and MINLATENCY. The static settings use static interrupt-timing values. The static values are not always optimal for all workload types or traffic patterns, and the static values cannot account for changes in traffic patterns.

There is also one supported dynamic setting (DYNAMIC). This setting causes the host (stack) to dynamically adjust the timer-interrupt value while the device is active and in use. This function exploits an OSA hardware function called Dynamic LAN Idle. Unlike the static settings, the DYNAMIC setting reacts to changes in traffic patterns and sets the interrupt-timing values to maximize throughput. The dynamic setting does not incur additional CPU consumption that might be produced when you specify any of the static settings. In addition, the DYNAMIC setting uses the OSA Dynamic Router Architecture function to enable QDIO inbound workload queues for specific inbound traffic types.

Result: When you specify OLM on the INTERFACE statement, the INBPERF parameter is ignored and the statement takes the value DYNAMIC.

Valid values for INBPERF are:

BALANCED
This setting uses a static interrupt-timing value, which is selected to achieve reasonably high throughput and reasonably low CPU consumption. This is the default value for CHPIDTYPE OSD. .

DYNAMIC
This setting causes the host to dynamically signal the OSA-Express feature to change the timer-interrupt value, based on current inbound workload conditions. The DYNAMIC setting is effective only for OSA-Express2 or later features on at least an IBM System z9 that supports the corresponding Dynamic LAN Idle function. See the 2097DEVICE Preventive Service Planning (PSP) bucket for more information about the OSA-Express3 adapter that supports this function. The DYNAMIC setting should outperform the other three static settings for most workload combinations. This is the default value for CHPIDTYPE OSX.

If the DYNAMIC setting is specified for an OSA-Express adapter that does not support the dynamic LAN Idle function, the stack reverts to using the BALANCED setting.

WORKLOADQ | NOWORKLOADQ

This subparameter controls the QDIO inbound workload queueing function for the interface. QDIO inbound workload queueing is effective only for OSA-Express features in QDIO mode that support the corresponding Data Router Architecture. OSA-Express features that support workload queueing do not necessarily support workload queueing for all possible traffic types. For more information about the QDIO inbound workload queueing function and the OSA-Express features that support it, see QDIO inbound workload queueing in z/OS Communications Server: IP Configuration Guide.

NOWORKLOADQ
Specifies that QDIO inbound workload queueing is not

enabled for inbound traffic. All inbound traffic for this interface uses a single input queue. This is the default value.

WORKLOADQ
Specifies that QDIO inbound workload queueing is enabled for inbound traffic.

If the WORKLOADQ subparameter is specified, QDIO inbound workload queueing is enabled for specific inbound traffic types. A primary input queue is reserved for all other traffic types.

Ancillary input queues (AIQs) are created for the following inbound traffic types when supported by the OSA-Express feature:

- Sysplex distributor
- Streaming workloads (for example FTP)
- Enterprise Extender (EE)

Requirement: You must specify the VMAC parameter with WORKLOADQ to enable QDIO inbound workload queueing.

If the WORKLOADQ setting is specified for an OSA-Express adapter that does not support the Data Router Architecture function, the stack reverts to using a single input queue.

MINCPU
This setting uses a static interrupt-timing value, which is selected to minimize host interrupts without regard to throughput. This mode of operation might result in minor queueing delays (latency) for packets flowing into the host, which is not optimal for workloads with demanding latency requirements.

MINLATENCY
This setting uses a static interrupt-timing value, which is selected to minimize latency (delay), by more aggressively sending received packets to the host. This mode of operation generally results in higher CPU consumption than the other three settings. Use this setting only if host CPU consumption is not an issue.

VMAC *macaddr*
Specifies the virtual MAC address, which can be represented by 12 hexadecimal characters. The OSA-Express device uses this address rather than the physical MAC address of the device for all IPv4 packets sent to and received from this TCP/IP stack. For CHPIDTYPE OSD, using a virtual MAC address is optional. For CHPIDTYPE OSX, using a virtual MAC address is required, so the VMAC parameter is the default

The *macaddr* value is optional. The *macaddr* value is optional for CHPIDTYPE OSD and cannot be specified for CHPIDTYPE OSX. If you do not code the *macaddr* value, then the OSA-Express device generates a virtual MAC address. If you do code the *macaddr* value, it must be defined as a locally administered individual MAC address. This means the MAC address must have bit 6 (the universal or local flag U bit) of the first byte set to 1 and bit 7 (the group or individual flag G bit) of the first byte set to 0. The second hexadecimal character must be 2, 6, A, or E. The bit positions within the 12 hexadecimal characters are indicated as follows:

```
|               1|1               3|3               4|
|0              5|6               1|2               7|
+----------------+----------------+----------------+
|xxxxxxUGxxxxxxxx|xxxxxxxxxxxxxxxx|xxxxxxxxxxxxxxxx|
+----------------+----------------+----------------+
```

Rules:

- The same virtual MAC address generated by the OSA-Express device during interface activation remains in effect for this OSA-Express for this TCP/IP stack, even if the interface is stopped or becomes inoperative (INOPs). A new virtual MAC address is generated only if the INTERFACE statement is deleted and redefined or if the TCP/IP stack is recycled.
- The NONROUTER, PRIROUTER, and SECROUTER parameters are ignored for an OSA-Express interface if the VMAC parameter is configured on the INTERFACE statement.

Guideline: Unless the virtual MAC address representing this OSA-Express device must remain the same even after TCP/IP termination and restart, configure VMAC without a *macaddr* value and allow the OSA-Express device to generate it. This guarantees that the VMAC address is unique from all other physical MAC addresses and from all other VMAC addresses generated by any OSA-Express feature.

ROUTEALL
Specifies that all IP traffic destined to the virtual MAC is forwarded by the OSA-Express device to the TCP/IP stack. This is the default value. See the router information in z/OS Communications Server: IP Configuration Guide for more details.

ROUTELCL
Specifies that only traffic destined to the virtual MAC and whose destination IP address is registered with the OSA-Express device by this TCP/IP stack is forwarded by the OSA-Express. See the router information in z/OS Communications Server: IP Configuration Guide for more details.

SMCR | NOSMCR
Specifies whether this interface can be used with Shared Memory Communications over Remote Direct Memory Access (SMC-R) for external data network communications.

NOSMCR
Specifies that this interface cannot be used for new TCP connections with SMC-R for external data network communications.

SMCR
Specifies that this interface can be used for new TCP connections with SMC-R for external data network communications. This is the default setting.

Rules:

- SMCR and NOSCMR are valid with CHPIDTYPE OSD definitions only.
- SMCR has no effect unless at least one Peripheral Component Interconnect Express (PCIe) function ID (PFID) value is specified by using the PFID subparameter of the SMCR parameter on the GLOBALCONFIG statement.
- SMCR has no effect unless a nonzero subnet mask is configured on the INTERFACE statement.

Guideline: If you enable Multipath and equal-cost interfaces are associated with different IP subnets, enabling SMC for some of, but not all, the interfaces can cause unpredictable SMC usage. You must specify either SMCR or NOSMCR on all equal-cost interfaces.

SMCD | NOSMCD
Specifies whether this interface can be used with Shared Memory Communications - Direct Memory Access (SMC-D).

NOSMCD
Specifies that this interface cannot be used for new TCP connections with SMC-D.

SMCD
Specifies that this interface can be used for new TCP connections with SMC-D. This is the default setting.

Rules:

- SMCD and NOSMCD are valid with CHPIDTYPE OSD definitions only.
- SMCD has no effect unless a nonzero subnet mask is configured on the INTERFACE statement.

Guideline: If you enable Multipath and equal-cost interfaces are associated with different IP subnets, enabling SMC for some of, but not all, the interfaces can cause unpredictable SMC usage. You must specify either SMCD or NOSMCD on all equal-cost interfaces.

SOURCEVIPAINTERFACE *vipa_name*
Specifies which previously-defined static VIPA interface is used for SOURCEVIPA (when IPCONFIG SOURCEVIPA is in effect). The *vipa_name* value is the interface name (or link name) for a VIRTUAL interface. This parameter is optional.

Requirement: The VIRTUAL interface must be defined prior to specifying this INTERFACE statement to the TCP/IP stack. It must either already be defined, or the INTERFACE statement (or DEVICE and LINK statements) that define the static VIPA must precede this INTERFACE statement in the profile data set.

Tip: The SOURCEVIPAINTERFACE setting can be overridden. See the information about Source IP address selection in z/OS Communications Server: IP Configuration Guide for the hierarchy of ways that the source IP address of an outbound packet is determined.

MTU *num*
The maximum transmission unit (MTU), in bytes. This value can be in the range 576 - 8992. The minimum MTU for IPv4 is 576. The stack takes the minimum of the configured value and the value supported by the device (returned by OSA).

The MTU default, which depends on the value that is supported by the device, is the following value:

- Gigabit Ethernet default MTU = 8992
- Fast Ethernet default MTU = 1492

The MTU default is 1492 for Fast Ethernet; otherwise, it is 8992.

Rule: If you are using OMPROUTE and OMPROUTE is not configured to ignore this interface, ensure that the MTU that you define on this parameter matches the MTU used by OMPROUTE for this interface. The MTU used by

OMPROUTE is the MTU value defined on the corresponding OMPROUTE statement (OSPF_INTERFACE, RIP_INTERFACE, or INTERFACE) for this interface. If an MTU value is not defined on the corresponding OMPROUTE statement for this interface or if no OMPROUTE statement is specified for this interface, the MTU used by OMPROUTE is the minimum MTU for IPv4 (576).

Tip: See z/OS Communications Server: IP Configuration Guide, in section Maximum transmission unit considerations, for additional information about how TCP/IP uses the MTU to determine the largest size frame to send.

READSTORAGE
An optional parameter indicating the amount of fixed storage that z/OS Communications Server should keep available for read processing for this adapter. Use the QDIOSTG VTAM start option to specify a value that applies to all OSA-Express adapters in QDIO mode. You can use the READSTORAGE keyword to override the global QDIOSTG value for this adapter based on the inbound workload that you expect over this interface on this stack. The valid values for READSTORAGE are:

GLOBAL
The amount of storage is determined by the QDIOSTG VTAM start option. This is the default value.

MAX Use this value if you expect a heavy inbound workload over this interface.

AVG Use this value if you expect a medium inbound workload over this interface.

MIN Use this value if you expect a light inbound workload over this interface.

Tip: See the description of the QDIOSTG VTAM start option in the z/OS Communications Server: SNA Resource Definition Reference for details about exactly how much storage is allocated by z/OS Communications Server for each of these values.

IPBCAST
Specifies that the interface both sends and receives IP broadcast packets. If this parameter is not specified, no IP broadcast packets are sent or received on this interface.

SECCLASS *security_class*
Use this parameter to associate a security class for IP filtering with this interface. For traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of 0. You can specify filter rules in the TCP/IP profile or in an IP security policy file that is read by the Policy Agent. Filter rules can include a security class specification on the IpService statement in an IP Security policy file or on the SECCLASS parameter on the IPSECRULE statement in the TCP/IP profile.

Valid security classes are identified as a number in the range 1 - 255. The default value is 255. For more information about security class values, see z/OS Communications Server: IP Configuration Guide.

The TCP/IP stack ignores this value if IPSECURITY is not specified on the IPCONFIG statement.

MONSYSPLEX | NOMONSYSPLEX
Specifies whether sysplex autonomics should monitor the interface's status.

NOMONSYSPLEX
Specifies that sysplex autonomics should not monitor the interface's status. This is the default value.

MONSYSPLEX
Specifies that sysplex autonomics should monitor the interface's status.

Restriction: The MONSYSPLEX attribute is not in effect unless the MONINTERFACE keyword is specified on the GLOBALCONFIG SYSPLEXMONITOR profile statement. The presence of dynamic routes over this interface is monitored if the DYNROUTE keyword is also specified on the GLOBALCONFIG SYSPLEXMONITOR profile statement.

DYNVLANREG | NODYNVLANREG
This parameter controls whether or not the VLAN ID for this interface is dynamically or statically registered with the physical switch on the LAN.

Restriction: This parameter is applicable only if a VLAN ID is specified on the statement.

Dynamic registration of VLAN IDs is handled by the OSA-Express feature and the physical switch on your LAN. Therefore, in order for the DYNVLANREG parameter to be effective, both must be at a level that provides the necessary hardware support for dynamic VLAN ID registration. After the interface is active, you can view the Netstat DEvlinks/**-d** report output to determine whether your OSA-Express feature can support VLAN dynamic registration. This Netstat report also displays whether dynamic VLAN ID registration has been configured for the interface.

NODYNVLANREG
Specifies that if a VLAN ID is configured for this interface, it must be manually registered with the physical switches on the corresponding LAN. This is the default value. If this parameter is specified without a VLAN ID, then it is ignored.

DYNVLANREG
Specifies that if a VLAN ID is configured for this interface, it is dynamically registered with the physical switches on the corresponding LAN. If this parameter is specified without a VLAN ID, then warning message EZZ0056I is issued and the NODYNVLANREG setting is used instead.

OLM | NOOLM
An optional parameter indicating whether an OSA-Express adapter operates in optimized latency mode.

NOOLM
Specifies that the OSA-Express adapter should not operate in optimized latency mode. This is the default value.

OLM Specifies that the OSA-Express adapter operates in optimized latency mode (OLM). Optimized latency mode optimizes interrupt processing for both inbound and outbound data. Use this mode for workloads that have demanding latency requirements. Because this mode can provide significant increases of throughput, particularly for interactive, non-streaming workloads. For more information about optimized latency mode, see the optimized latency mode topic in z/OS Communications Server: IP Configuration Guide.

Guidelines:

- Because of the operating characteristics of optimized latency mode, you might need to change your configuration to direct traffic to particular OSA-Express write priority queues and to limit the number of concurrent users sharing an OSA-Express configured for optimized latency mode. For more information about OLM, see the optimized latency mode topic in z/OS Communications Server: IP Configuration Guide.
- The optimized latency mode function targets a z/OS environment with a high-volume, interactive workloads. Although optimized latency mode can compensate for some mixing of workloads, an excessive amount of high-volume streaming workloads, such as bulk data or file transfer, can result in higher CPU consumption.

Restrictions:

- This function is limited to OSA-Express3 or later Ethernet features in QDIO mode that are running with an IBM System z10 or later. See the 2097 DEVICE Preventive Service Planning (PSP) bucket for more information.
- Traffic that is either inbound over or being forwarded to an OSA-Express configured to use optimized latency mode is not eligible for the accelerated routing function provided by HiperSockets Accelerator and QDIO Accelerator.
- For an OSA-Express configured to use optimized latency mode, the stack ignores the configured or default INBPERF setting and uses the value DYNAMIC.

ISOLATE | NOISOLATE

Specifies whether packets should be directly routed between TCP/IP stacks that share the OSA adapter.

NOISOLATE

Route packets directly between TCP/IP stacks sharing the OSA adapter. In this mode, if the next hop address was registered by another stack that is sharing the OSA adapter, then the OSA-Express adapter routes the packet directly to the sharing stack without putting the packet on the external LAN.

ISOLATE

Prevent OSA-Express from routing packets directly to another TCP/IP stack that is sharing the OSA adapter. In this mode, OSA-Express adapter discards any packets when the next hop address was registered by another stack that is sharing the OSA adapter. Packets can flow between two stacks that share the OSA only by first going through a router on the LAN. For more details, see the OSA-Express connection isolation information in z/OS Communications Server: IP Configuration Guide.

Tips:

- If you isolate an interface, there might be an adverse effect on latency.
- You can selectively apply OSA-Express connection isolation to individual virtual LANs.
- The OSA-Express adapter requires that both stacks sharing the port be non-isolated for direct routing to occur. Therefore, for traffic between two stacks sharing the OSA adapter, as long as at least one of the stacks is isolated, connection isolation is in effect for traffic in both directions between these stacks.

Restriction: This function is limited to OSA-Express2 or later Ethernet features in QDIO mode and running at least an IBM System z9 Enterprise Class (EC) or z9 Business Class (BC). See the 2094DEVICE, 2096DEVICE, 2097DEVICE, or 2098DEVICE Preventive Service Planning (PSP) bucket for more information.

Steps for modifying

See Summary of INTERFACE statements for modification information.

Examples

```
INTERFACE OSAQDIO24
DEFINE IPAQENET
PORTNAME OSAQDIO2
SOURCEVIPAINT VIPAV4
IPADDR 100.1.1.1/24
```

Related topics

- BEGINROUTES statement
- BSDROUTINGPARMS statement
- DEVICE and LINK - MPCIPA OSA-Express QDIO devices statement
- "GLOBALCONFIG statement" on page 55
- "INTERFACE - IPAQENET6 OSA-Express QDIO interfaces statement" on page 95
- SACONFIG statement
- START statement
- STOP statement

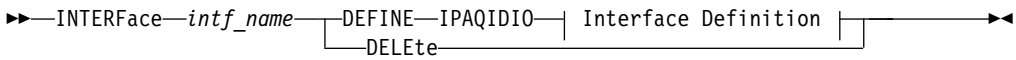
INTERFACE - IPAQIDIO HiperSockets interfaces statement

Use the INTERFACE statement for IPAQIDIO to configure IPv4 HiperSockets connectivity. Use the CHPID parameter to specify the value of the desired IQD CHPID that was configured within HCD. HiperSockets interfaces do not require a corresponding TRLE definition. Instead, the TRLE is dynamically built when the interface is started.

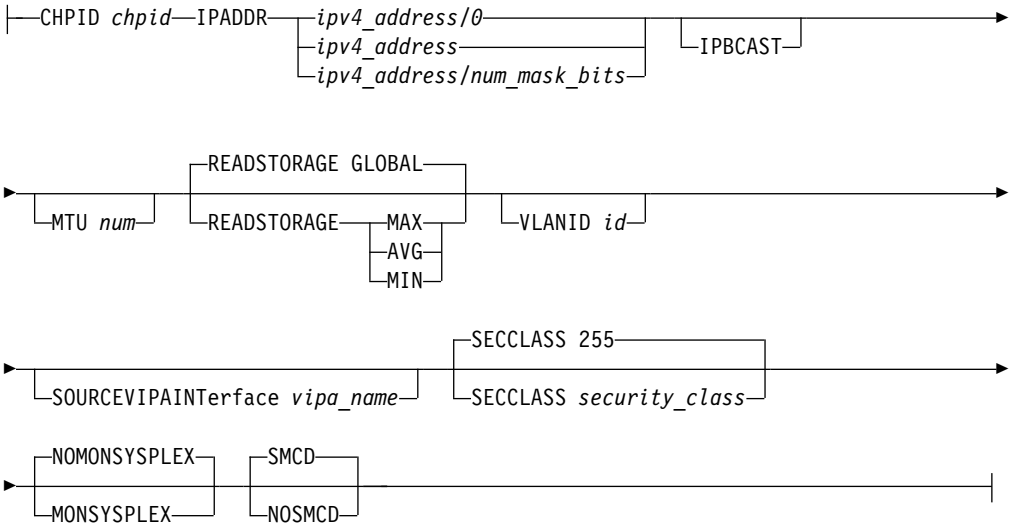
To determine the HiperSockets microcode level, use the DISPLAY TRL command. If a specific HiperSockets function is documented with a minimum microcode level, you can use this command to determine whether that function is supported. IBM service might request the microcode level for problem diagnosis. For more information, see DISPLAY TRL command in z/OS Communications Server: SNA Operation.

Rule: Specify the required parameters in the order shown here. The Interface Definition parameters can be specified in any order.

Syntax



Interface Definition:



Parameters

intf_name
The name of the interface. The maximum length is 16 characters.

DEFINE
Specifies that this definition is to be added to the list of defined interfaces.

DELETE
Specifies that this definition is to be deleted from the list of defined interfaces. The *intf_name* must be the name of an interface that was previously defined by an INTERFACE statement. INTERFACE DELETE deletes the home IP address for the interface.

IPAQIDIO
Indicates that the interface is for HiperSockets IPv4.

CHPID *chpid*
Use this parameter to specify the IQD CHPID for the HiperSockets interface. This value is a 2-character hexadecimal value (00x - FFx). The hexadecimal value specified on the CHPID parameter cannot be the same value that is used for the dynamic XCF HiperSockets interface. See the IQDCHPID start option in the z/OS Communications Server: SNA Resource Definition Reference.

IPADDR *ipaddr_spec*

ipv4_address
The home IP address for this interface.

Requirement: The IP address must be specified in dotted decimal form.

num_mask_bits
An integer value in the range 0 - 32 that represents the number of leftmost significant bits for the subnet mask of the interface. The default is 0.

Requirement: If you are configuring multiple IPv4 VLAN interfaces to the same HiperSockets CHPID, then you must specify a nonzero value

for the *num_mask_bits* variable for each of these interfaces and the resulting subnet must be unique for each of these interfaces.

Rule: If you are using OMPROUTE and OMPROUTE is not configured to ignore this interface, ensure that the subnet mask value that you define on this parameter matches the subnet mask used by OMPROUTE for this interface. The subnet mask used by OMPROUTE is the subnet mask value defined on the corresponding OMPROUTE statement (OSPF_INTERFACE, RIP_INTERFACE, or INTERFACE) for this interface. If no OMPROUTE statement is specified for this interface, the subnet mask used by OMPROUTE is the class mask for the interface IP address.

IPBCAST
Specifies that the interface both sends and receives IP broadcast packets. If this parameter is not specified, no IP broadcast packets are sent or received on this interface.

MTU *num*
The maximum transmission unit (MTU), in bytes. This value can be in the range 576 - 57344. The minimum MTU for IPv4 is 576. The stack takes the minimum of the configured value and the firmware supported value (which is the IQD frame size configured in HCD minus 8192)

The MTU default is equal to the IQD frame size minus 8192.

Rule: If you are using OMPROUTE and OMPROUTE is not configured to ignore this interface, ensure that the MTU that you define on this parameter matches the MTU used by OMPROUTE for this interface. The MTU used by OMPROUTE is the MTU value defined on the corresponding OMPROUTE statement (OSPF_INTERFACE, RIP_INTERFACE, or INTERFACE) for this interface. If an MTU value is not defined on the corresponding OMPROUTE statement for this interface or if no OMPROUTE statement is specified for this interface, the MTU used by OMPROUTE is the minimum MTU for IPv4 (576).

Tip: See Determining the maximum transmission unit in z/OS Communications Server: IP Configuration Guide for more information about how TCP/IP uses the MTU to determine the largest size frame to send.

READSTORAGE
An optional parameter that indicates the amount of fixed storage that z/OS CS should keep available for read processing for this interface. The IQDIOSTG VTAM start option allows you to specify a value that applies to all HiperSockets interfaces. You can use the READSTORAGE keyword to override the global IQDIOSTG value for this interface based on the inbound workload that you expect over this interface on this stack. The following values are valid:

GLOBAL
The amount of storage is determined by the IQDIOSTG VTAM start option. This is the default value.

MAX
Use this value if you expect a heavy inbound workload over this interface.

AVG
Use this value if you expect a medium inbound workload over this interface.

MIN
Use this value if you expect a light inbound workload over this interface.

Tip: See the description of the IQDIOSTG VTAM start option in the z/OS Communications Server: SNA Resource Definition Reference for details about exactly how much storage is allocated by z/OS Communications Server for each of these values.

VLANID *id*
An optional parameter followed by a decimal number indicating the virtual LAN identifier to be assigned to this HiperSockets interface. The valid range is 1 - 4 094.

SOURCEVIPAINTERFACE *vipa_name*
An optional parameter used to specify which previously-defined VIPA interface is to be used for SOURCEVIPA (when IPCONFIG SOURCEVIPA is in effect). The *vipa_name* value is the interface name for a VIRTUAL interface.

Requirement: The VIRTUAL interface or the link must be defined prior to specifying this INTERFACE statement to the TCP/IP stack. It must either already be defined, or the INTERFACE statement (or DEVICE and LINK statements) that define the static VIPA must precede this INTERFACE statement in the profile data set.

Tip: The use of the SOURCEVIPAINTERFACE parameter can be overridden. See the information about Source IP address selection in z/OS Communications Server: IP Configuration Guide for the hierarchy of ways that the source IP address of an outbound packet is determined.

SECCLASS *security_class*
Use this parameter to associate a security class for IP filtering with this interface. For traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of 0. Filter rules can be specified in the TCP/IP profile or in an IP Security policy file that is read by the Policy Agent. Filter rules can include a security class specification on the IpService statement in an IP Security policy file or on the SECCLASS parameter on the IPSECRULE statement in the TCP/IP profile.

Valid security classes are identified as a number in the range 1 - 255. The default value is 255. See security class values in z/OS Communications Server: IP Configuration Guide for more information.

Restriction: The TCP/IP stack ignores this value if IPSECURITY is not specified on the IPCONFIG statement.

MONSYSPLEX | NOMONSYSPLEX
Specifies whether or not sysplex autonomics should monitor the interface's status.

NOMONSYSPLEX
Specifies that sysplex autonomics should not monitor the interface's status. This is the default value.

MONSYSPLEX
Specifies that sysplex autonomics should monitor interface's status.

Restriction: The MONSYSPLEX attribute is not in effect unless the MONINTERFACE keyword is specified on the GLOBALCONFIG SYSPLEXMONITOR profile statement. The presence of dynamic routes over the interface is monitored if the DYNROUTE keyword is also specified on the GLOBALCONFIG SYSPLEXMONITOR profile statement.

SMCD | NOSMCD
Specifies whether this interface can be used with Shared Memory Communications - Direct Memory Access (SMC-D).

NOSMCD
Specifies that this interface cannot be used for new TCP connections with SMC-D.

SMCD
Specifies that this interface can be used for new TCP connections with SMC-D. This is the default setting.

Rule: SMCD has no effect unless a nonzero subnet mask is configured on the INTERFACE statement.

Guideline: If you enable Multipath and equal-cost interfaces are associated with different IP subnets, enabling SMC for some of, but not all, the interfaces can cause unpredictable SMC usage. You must specify either SMCD or NOSMCD on all equal-cost interfaces.

Steps for modifying

See Summary of INTERFACE statements for modification information.

Examples

```
INTERFACE HIPERSOCK1 DEFINE IPAQIDIO CHPID FC
             IPADDR 9.1.1.1/24
```

Related topics

- BEGINROUTES statement
- DEVICE and LINK — MPCIPA HiperSockets devices statement
- "INTERFACE - IPAQIDIO6 HiperSockets interfaces statement" on page 111
- START statement
- STOP statement

INTERFACE - IPAQENET6 OSA-Express QDIO interfaces statement

Use the INTERFACE statement to specify an OSA-Express QDIO Ethernet interface for IPv6.

To determine the OSA-Express microcode level, use the DISPLAY TRL command. If a specific OSA-Express function is documented with a minimum microcode level, you can use this command to determine whether that function is supported. IBM service might request the microcode level for problem diagnosis. For more information about the DISPLAY TRL command, see z/OS Communications Server: SNA Operation.

The following OSA-Express features can be defined in QDIO mode for IPv6:

- Fast Ethernet
- Gigabit Ethernet
- 1000BASE-T Ethernet
- 10G Ethernet

When you start an IPAQENET6 interface (and you do not specify VMAC with ROUTEALL), TCP/IP registers all non-loopback local (home) IPv6 addresses for this TCP/IP instance to the OSA-Express feature. If you subsequently add, delete, or change any home IPv6 addresses on this TCP/IP instance, TCP/IP dynamically registers the changes to the OSA-Express feature. If stateless address autoconfiguration is enabled for this interface, TCP/IP dynamically registers autoconfigured addresses to the OSA-Express feature. This includes both public and temporary autoconfigured addresses. The OSA-Express feature routes datagrams destined to those IPv6 addresses to this TCP/IP instance.

If a datagram is received by the OSA adapter for an unregistered IPv6 address, then the OSA-Express feature routes the datagram to the TCP/IP instance, depending on the setting of a virtual MAC (VMAC) address or whether the definition of an instance is PRIROUTER or SECROUTER. If the datagram is not destined for a virtual MAC address and no active TCP/IP instance using this interface is defined as PRIROUTER or SECROUTER, then the OSA-Express feature discards the datagram. For more details about the OSA-Express feature routing considerations, see the router information in z/OS Communications Server: IP Configuration Guide and primary and secondary routing in z/OS Communications Server: SNA Network Implementation Guide.

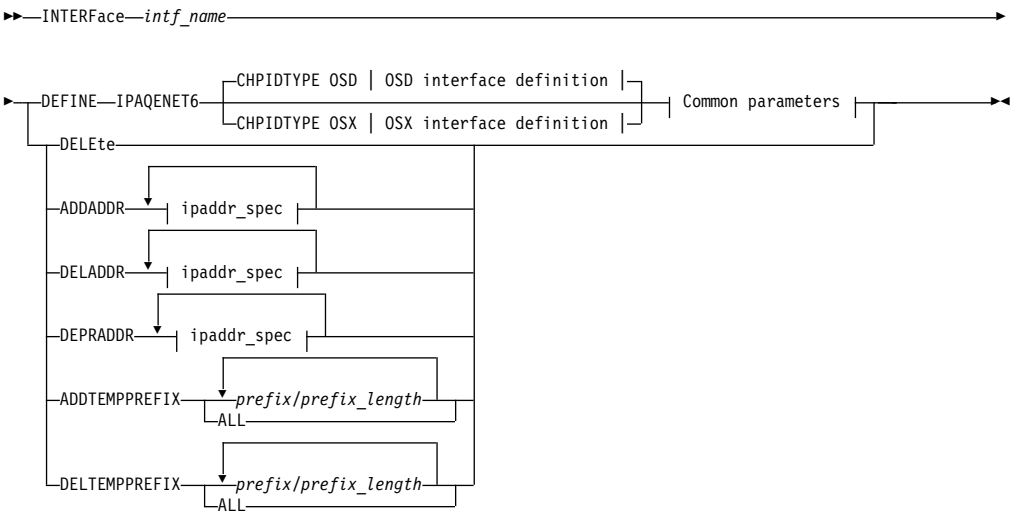
For detailed instructions on setting up an OSA-Express feature, see zEnterprise System and System z10 OSA-Express Customer's Guide and Reference.

For more information about missing interrupt handler (MIH) considerations with TCP/IP interfaces, see Missing interrupt handler factors.

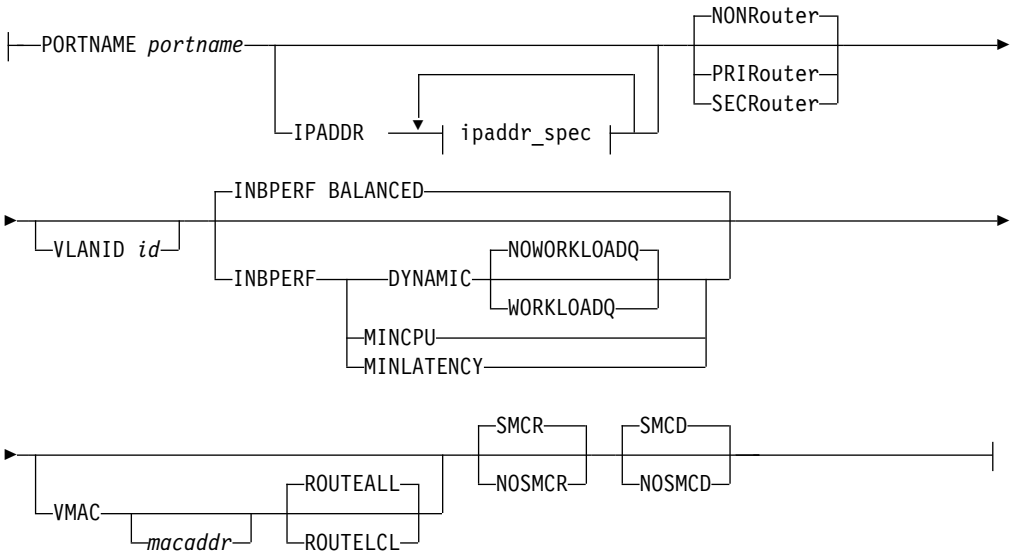
Restriction: This statement applies to IPv6 IP addresses only.

Syntax

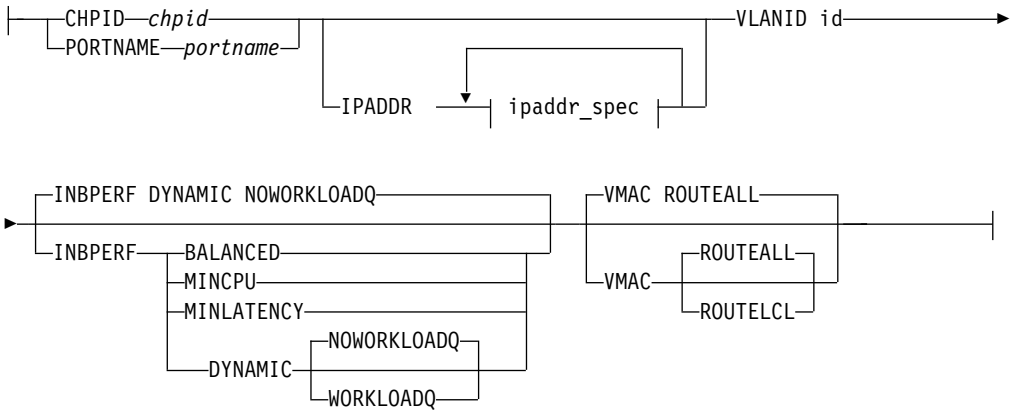
Rule: Specify the required parameters and the CHPIDTYPE parameter in the order shown here. The OSD Interface Definition and OSX Interface Definition parameters can be specified in any order.



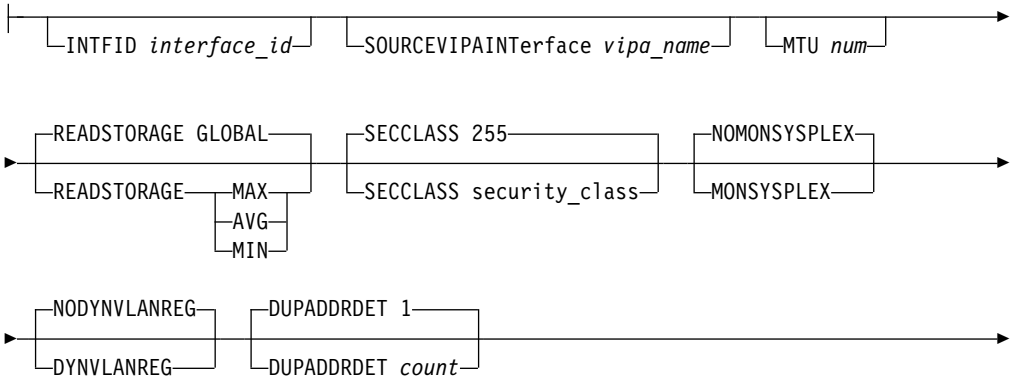
OSD interface definition:

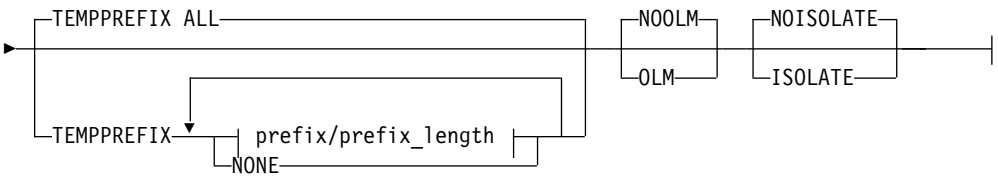


OSX Interface definition:

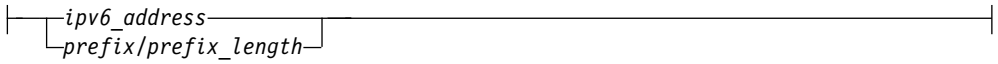


Common parameters for OSD and OSX interface definitions:





ipaddr_spec:



Parameters

intf_name
The name of the interface. The maximum length is 16 characters.

Requirement: This name must be different than the name specified for the PORTNAME parameter.

Restriction: Do not specify the value PUBLICADDRS or TEMPADDRS for the interface name. The values PUBLICADDRS and TEMPADDRS are keywords on the SRCIP statement. These values are not recognized if they are specified as an IPv6 interface name on an SRCIP entry.

DEFINE
Specifies that this definition is to be added to the list of defined interfaces.

DELETE
Specifies that this definition is to be deleted from the list of defined interfaces. The *intf_name* must be the name of an interface previously defined by an INTERFACE statement. INTERFACE DELETE deletes all home IP addresses for the interface.

CHPIDTYPE
An optional parameter indicating the CHPID type of the OSA-Express QDIO interface.

OSD The external data network. This is the default value.

OSX The intraensemble data network. See z/OS Communications Server: IP Configuration Guide for information about requirements necessary to make an OSX work.

Rule: You must specify an OSD interface definition to make this OSA-Express QDIO interface eligible to use Shared Memory Communications over Remote Direct Memory Access (SMC-R) or Shared Memory Communications - Direct Memory Access (SMC-D).

IPADDR *ipaddr_spec*
For information about the IPv6 address restrictions, see Restrictions on IPv6 addresses configured in the TCP/IP profile.

The following value can be specified for *ipaddr_spec*:

ipv6_address

This parameter can be one of the following values:

- ipv6_addr (A fully qualified IPv6 address is in colon-hexadecimal format.)

- prefix/64 [The digits (in colon-hexadecimal format) before the / represent the prefix. The prefix length represents the length of the prefix in bits. If a prefix length is coded, it must be equal to 64. When a prefix is specified, TCP/IP constructs the IPv6 address by appending the interface ID to it.]

Restriction: If you code a prefix that is longer than 64 bits, it is truncated to 64 bits, and no error messages are issued.

ADDADDR *ipaddr_spec*
Allows the addition of IP addresses to an existing INTERFACE definition (similar to updating the HOME list with the VARY TCPIP,,OBEYFILE command) without having to delete and redefine the INTERFACE. This can be used to change the autoconfiguration state of an interface. If ADDADDR is coded and this is the first manually configured IP address for the interface, then TCP/IP disables autoconfiguration for the interface. The *intf_name* coded with ADDADDR must be the name of an interface previously defined by an INTERFACE statement.

Any public or temporary addresses that had previously been autoconfigured for the interface are deleted.

DELADDR *ipaddr_spec*
Allows you to delete IP addresses from an existing INTERFACE definition. If DELADDR is coded for the last or only manually configured IP address for an interface, then TCP/IP enables autoconfiguration for the interface. DELADDR is valid only for an IP address or prefix configured manually. The *intf_name* coded with DELADDR must be the name of an interface previously defined by an INTERFACE statement. DELADDR is valid only in a data set specified on a VARY TCPIP,,OBEYFILE command.

Guideline: If you specify a prefix for DELADDR, then the only IP addresses affected are those defined by way of the same prefix specified on IPADDR or ADDADDR.

DEPRADDR *ipaddr_spec*
The DEPRADDR keyword allows you to deprecate an IP address. This can assist with site renumbering. DEPRADDR is valid only for an IP address or prefix configured manually. If you use DEPRADDR to deprecate an IP address, you can subsequently use ADDADDR again to make that IP address preferred. For DEPRADDR, the *interface_name* must be the name of an interface previously defined by an INTERFACE statement. DEPRADDR is valid only in a data set specified on a VARY TCPIP,,OBEYFILE command.

Guideline: If you specify a prefix for DEPRADDR, then the only IP addresses affected are those defined by way of the same prefix specified on IPADDR or ADDADDR.

ADDTEMPPREFIX
Use the ADDTEMPPREFIX keyword to add prefixes to the temporary prefixes list of an existing INTERFACE definition without having to delete and redefine the INTERFACE statement. The temporary prefixes list limits the set of prefixes for which temporary IPv6 addresses can be generated. A temporary IPv6 address is generated when a router advertisement containing the prefix is processed, and the prefix is included in one of the prefixes in the temporary prefixes list. For example, if the temporary prefixes list for an interface contains a single prefix 2001:0db8:58cd::/48, a temporary address is generated for advertised prefix 2001:0db8:58cd:0001/64; however, a temporary address is not generated on this interface for advertised prefix 2001:0db8:5555:0001/64. The

intf_name variable coded with ADDTEMPPREFIX must be the name of an interface that was previously defined by an INTERFACE statement.

prefix/prefix_length
The digits (in colon-hexadecimal format) before the slash (/) represent the prefix. The *prefix_length* value represents the length of the prefix in bits. Valid values for *prefix_length* parameter are in the range 1 - 64.

ALL Causes temporary addresses to be generated for all prefixes that are learned over this interface by way of router advertisements.

DELTEMPPREFIX
Use the DELTEMPPREFIX keyword to delete prefixes from the temporary prefixes list of an existing INTERFACE definition. The temporary prefixes list limits the set of prefixes for which temporary IPv6 addresses can be generated. A temporary IPv6 address is generated when a router advertisement containing the prefix is processed and the prefix is included in one of the prefixes in the temporary prefixes list. The *intf_name* variable coded with the DELTEMPPREFIX keyword must be the name of an interface that was previously defined by an INTERFACE statement.

prefix/prefix_length
The digits (in colon-hexadecimal format) before the slash (/) represent the prefix. The *prefix_length* value represents the length of the prefix in bits. Valid values for the *prefix_length* are in the range 1 - 64. All temporary addresses for this interface whose prefix is not included in the updated temporary prefixes list are deleted.

ALL Delete all prefixes from the temporary prefixes list, which sets the temporary prefixes list to NONE. All temporary addresses for this interface are deleted, and no more temporary addresses are generated for this interface.

IPADDR *ipaddr_spec*
TCP/IP always creates the link-local IPv6 address. If IPADDR is not specified, then TCP/IP enables autoconfiguration for the interface.

Tip: Autoconfiguration is enabled if there is a router or some other device that provides a router advertisement.

If no address or prefix is specified, it is obtained from a router on the LAN by way of an IPv6 stateless autoconfiguration. For more information, see z/OS Communications Server: IPv6 Network and Application Design Guide.

IPAQENET6
Indicates that the interface uses the interface based on IP assist, belongs to the QDIO family of interfaces, and uses the Gigabit Ethernet or Fast Ethernet protocol.

INTFID *interface_id*
An optional 64-bit interface identifier in colon-hexadecimal format. IPv6 shorthand is not allowed when specifying the interface ID. If specified, this interface ID is used to form the link-local address for the interface, and is also appended to any manually configured prefixes for the interface, to form complete IPv6 addresses on the interface. If you do not configure manual IP addresses on the interface, the INTFID value is appended to any prefixes that are learned over this interface by way of router advertisements to form public IPv6 addresses on the interface. The INTFID value is not used to form temporary IPv6 addresses. A randomly generated interface ID is appended to any learned prefixes to form temporary IPv6 addresses on the interface (if temporary addresses are enabled).

If INTFID is not coded, TCP/IP builds the Interface ID using information returned from the OSA-Express Adapter (during Interface activation). The built Interface ID value is then used to form the link-local address. This value is also used to complete the formation of other IPv6 addresses on the interface, if you choose to configure only the prefix portion of the addresses (by way of IPADDR or ADDADDR). Also, if you do not configure manual IP addresses on the interface, the built interface ID value is appended to any prefixes learned over this interface by way of router advertisements to form public IPv6 addresses on the interface. The built interface ID value is not used to form temporary IPv6 addresses. A randomly generated interface ID is appended to any learned prefixes to form temporary IPv6 addresses on the interface (if temporary addresses are enabled).

When defining the interface ID, the local/universal flag (the U bit, bit 6 shown in the following example) must be set to 0. The group/individual flag (the G bit, bit 7 shown in the following example) must also be set to 0. If either flag is set incorrectly, interface definition fails. Additionally, an interface ID value correlating to an ISATAP address or a Reserved Anycast address is not allowed. (An ISATAP Interface ID has '00005EFE'x in bits 0 - 31, and a Reserved Anycast Interface ID has 'FCFFFFFFFFFFFF8' in bits 0 - 56.)

```
|               1|1               3|3               4|4               6|
|0              5|6               1|2               7|8               3|
+----------------+----------------+----------------+----------------+
|xxxxxxUGxxxxxxxx|xxxxxxxxxxxxxxxx|xxxxxxxxxxxxxxxx|xxxxxxxxxxxxxxxx|
+----------------+----------------+----------------+----------------+
```

SOURCEVIPAINTERFACE *vipa_name*

SOURCEVIPAINTERFACE is optional. Use this parameter to specify which previously defined static VIPA interface is to be used for SOURCEVIPA (when IPCONFIG6 SOURCEVIPA is in effect).

Tip: The use of the SOURCEVIPAINTERFACE parameter can be overridden. See the information about source IP address selection in z/OS Communications Server: IP Configuration Guide for the hierarchy of ways that the source IP address of an outbound packet is determined.

The *vipa_name* is the interface name for a VIRTUAL6 interface. If the VIPA has multiple IP addresses, then the sourcevipa address for outbound packets is selected from among these addresses according to the default source address selection algorithm. For more information, seez/OS Communications Server: IPv6 Network and Application Design Guide.

Requirement: The VIRTUAL6 interface must be defined prior to specifying this INTERFACE statement to the TCP/IP stack. It must either already be defined or, the INTERFACE statement that defines it must precede this INTERFACE statement in the profile data set.

CHPID *chpid*

This parameter applies only to interfaces of CHPIDTYPE OSX and is used to specify the CHPID for the interface. This value is a 2-character hexadecimal value (00 - FF).

PORTNAME *portname*

Use this parameter to specify the PORT name contained in the TRLE definition for the QDIO interface. The TRLE must be defined as MPCLEVEL=QDIO. For details about defining a TRLE, see z/OS Communications Server: SNA Resource Definition Reference.

Requirement: The *portname* value must be different from the name that is specified for the *intf_name* value.

NONROUTER
If a datagram is received at this interface for an unknown IP address, the datagram is not routed to this TCP/IP instance. This is the default value.

PRIRouter and SECRouter parameters interact with the VLANID parameter. See the VLANID parameter to understand this relationship.

For more information about VLANID parameter interactions, see z/OS Communications Server: IP Configuration Guide.

Rule: This keyword applies only to interfaces of CHPIDTYPE OSD and is ignored if the VMAC parameter is configured on the INTERFACE statement.

PRIROUTER
If a datagram is received at this interface for an unknown IP address and is not destined for a virtual MAC, the datagram is routed to this TCP/IP instance.

Rule: This keyword applies only to interfaces of CHPIDTYPE OSD and is ignored if the VMAC parameter is configured on the INTERFACE statement.

SECROUTER
If a datagram is received at this interface for an unknown IP address and is not destined for a virtual MAC, and there is no active TCP/IP instance defined as PRIROUTER, then the datagram is routed to this TCP/IP instance.

Rule: This keyword applies only to interfaces of CHPIDTYPE OSD and is ignored if the VMAC parameter is configured on the INTERFACE statement.

DUPADDRDET *count*
Use this parameter to specify the number of times to attempt duplicate address detection. The minimum value is 0, maximum is 2 and default is 1. This is an optional parameter.

Guideline: A value of 0 means that TCP/IP does not perform duplicate address detection for this interface.

MTU *num*
The maximum transmission unit (MTU) in bytes. This value can be up to 9000. The minimum MTU for IPv6 is 1280. The stack takes the minimum of the configured value and the value supported by the device (returned by the OSA adapter).

The MTU default, which depends on value supported by device, is the following value:

- Gigabit Ethernet default MTU = 9000
- Fast Ethernet default MTU = 1500

Tip: See z/OS Communications Server: IP Configuration Guide, in section Maximum transmission unit considerations, for additional information about how TCP/IP uses the MTU to determine the largest size frame to send.

VLANID id
Specifies the decimal virtual LAN identifier to be assigned to the OSA-Express INTERFACE. This field should be a virtual LAN identifier recognized by the switch for the LAN connected to this OSA-Express. The valid range is 1 - 4094. This parameter is optional for CHPIDTYPE OSD and required for CHPIDTYPE OSX.

Guideline: Installation configuration on other platforms or related to Ensemble networking can limit the maximum VLANID of 4096.

The VLANID parameter interacts with the PRIRouter and SECRouter parameters. If you configure both the VLANID parameter and either

PRIROUTER or SECROUTER parameter, then this TCP/IP instance acts as a router for this VLAN (ID) only. Datagrams that are received at this device instance for an unknown IP address and are not destined for a virtual MAC are routed only to this TCP/IP instance if it is VLAN tagged with this VLAN ID. For more information about VLANID parameter interactions, see z/OS Communications Server: IP Configuration Guide.

Rule: If you are configuring multiple VLAN interfaces to the same OSA-Express feature, then you must specify the VMAC parameter (with the default ROUTEALL attribute) on the INTERFACE statement for each of these interfaces.

Restriction: The stack supports a maximum of 32 IPv6 VLAN interfaces to the same OSA-Express port. Additional VLANID limitations might exist if this interface can be used with Shared Memory Communications over Remote Direct Memory Access (SMC-R). See VLANID considerations in z/OS Communications Server: IP Configuration Guide for details.

READSTORAGE

An optional parameter indicating the amount of fixed storage that z/OS Communications Server should keep available for read processing for this adapter. The QDIOSTG VTAM start option allows you to specify a value which applies to all OSA-Express adapters in QDIO mode. You can use the READSTORAGE keyword to override the global QDIOSTG value for this adapter based on the inbound workload you expect over this interface on this stack. The valid values are:

GLOBAL
The amount of storage is determined by the QDIOSTG VTAM start option. This is the default value.

MAX Use this value if you expect a heavy inbound workload over this interface.

AVG Use this value if you expect a medium inbound workload over this interface.

MIN Use this value if you expect a light inbound workload over this interface.

Tip: See the description of the QDIOSTG VTAM start option in the z/OS Communications Server: SNA Resource Definition Reference for details about exactly how much storage is allocated by z/OS Communications Server for each of these values.

Rule: If you define both a LINK and INTERFACE statement for the same adapter, then the READSTORAGE value on the LINK statement must match the READSTORAGE value on the corresponding INTERFACE statement. If you define an INTERFACE statement that contains a value for READSTORAGE that conflicts with the READSTORAGE value for a previous LINK statement for the same adapter, then TCP/IP rejects the INTERFACE statement.

INBPERF

An optional parameter that indicates how processing of inbound traffic for the QDIO interface is performed.

There are three supported static settings (MINCPU, MINLATENCY, and BALANCED).that indicate how frequently the adapter should interrupt the host for inbound traffic: BALANCED, MINCPU, and MINLATENCY. The static

settings use static interrupt-timing values. The static values are not always optimal for all workload types or traffic patterns, and cannot account for changes in traffic patterns.

There is also one supported dynamic setting (DYNAMIC). This setting causes the host (stack) to dynamically adjust the timer-interrupt value while the device is active and in use. This function exploits an OSA hardware function called Dynamic LAN Idle. Unlike the static settings, the DYNAMIC setting reacts to changes in traffic patterns, and sets the interrupt-timing values at the point where throughput is maximized. In addition, the DYNAMIC setting uses the OSA Dynamic Router Architecture function to enable QDIO inbound workload queues for specific inbound traffic types.

Result: When you specify OLM on the INTERFACE statement, the INBPERF parameter is ignored and the statement defaults to the value DYNAMIC.

Valid values are:

BALANCED
This setting uses a static interrupt-timing value, which is selected to achieve reasonably high throughput and reasonably low CPU consumption. This is the default value for CHPIDTYPE OSD.

DYNAMIC
This setting causes the host to dynamically signal the OSA-Express feature to change the timer-interrupt value, based on current inbound workload conditions. The DYNAMIC setting is effective only for OSA-Express2 or later features on at least an IBM System z9 that supports the corresponding Dynamic LAN Idle function. See the 2094DEVICE Preventive Service Planning (PSP) bucket and the 2096DEVICE Preventive Service Planning (PSP) bucket for more information about the level of OSA-Express2 adapter that supports this function. See the 2097DEVICE Preventive Service Planning (PSP) bucket for more information about the OSA-Express3 adapter that supports this function. The DYNAMIC setting can decrease latency and provide increases in throughput for many interactive workloads. For all other workload combinations, this setting provides performance similar to the three static settings. This is the default value for CHPIDTYPE OSX.

If the DYNAMIC setting is specified for an OSA-Express adapter that does not support the dynamic LAN Idle function, the stack reverts to using the BALANCED setting.

WORKLOADQ | NOWORKLOADQ

This subparameter controls the QDIO inbound workload queueing function for the interface. QDIO inbound workload queueing is effective only for OSA-Express features in QDIO mode that support the corresponding Data Router Architecture. OSA-Express features that support workload queueing do not necessarily support workload queueing for all possible traffic types. For more information about the QDIO inbound workload queueing function and the OSA-Express features that support it, see QDIO inbound workload queueing in z/OS Communications Server: IP Configuration Guide.

NOWORKLOADQ
Specifies that QDIO inbound workload queueing is not

enabled for inbound traffic. All inbound traffic for this interface uses a single input queue. This is the default.

WORKLOADQ
Specifies that QDIO inbound workload queueing is enabled for inbound traffic.

If the WORKLOADQ subparameter is specified, QDIO inbound workload queueing is enabled for specific inbound traffic types. A primary input queue is reserved for all other traffic types.

Ancillary input queues (AIQs) are created for the following inbound traffic types when supported by the OSA-Express feature:

- Sysplex distributor
- Streaming workloads (for example FTP)
- Enterprise Extender (EE)

Requirement: You must specify the VMAC parameter with WORKLOADQ to enable QDIO inbound workload queueing.

If the WORKLOADQ setting is specified for an OSA-Express adapter that does not support the Data Router Architecture function, the stack reverts to using a single input queue.

MINCPU
This setting uses a static interrupt-timing value, which is selected to minimize host interrupts without regard to throughput. This mode of operation might result in minor queueing delays (latency) for packets into the host, which is not optimal for workloads with demanding latency requirements.

MINLATENCY
This setting uses a static interrupt-timing value, which is selected to minimize latency (delay), by more aggressively presenting received packets to the host. This mode of operation generally results in higher CPU consumption than the other three settings. Use this setting only if host CPU consumption is not an issue.

Rule: If you define both a LINK IPAQENET and an INTERFACE IPAQENET6 statement for the same adapter, then the following rules apply for the INBPERF parameter on these statements:

- The value on the LINK statement must match the INBPERF value on the corresponding INTERFACE statement.
- The INTERFACE statement supports the subparameters WORKLOADQ and NOWORKLOADQ for the INBPERF DYNAMIC parameter. These subparameters are associated with QDIO inbound workload queueing support and are not supported on the LINK IPAQENET statement. So, if you specify the INBPERF DYNAMIC parameter for both the LINK and the INTERFACE statements, then you must use the default or specify the NOWORKLOADQ subparameter for the INBPERF DYNAMIC parameter on the INTERFACE statement. This ensures that the INBPERF DYNAMIC setting for both statements is the same.

- If you define an INTERFACE IPAQENET6 statement that contains a value for INBPERF that conflicts with the INBPERF value for a previous LINK IPAQENET statement for the same adapter, then TCP/IP rejects the INTERFACE statement.

SECCLASS *security_class*
Use this parameter to associate a security class for IP filtering with this interface. In order for traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of 0. Filter rules can be specified in the TCP/IP profile or in an IP Security policy file read by the Policy Agent. Filter rules can include a security class specification on the IpService statement in an IP Security policy file or on the SECCLASS parameter on the IPSEC6RULE statement in the TCP/IP profile.

Valid security classes are identified as a number in the range 1 - 255. The default value is 255. For more information about security class values, see z/OS Communications Server: IP Configuration Guide.

The TCP/IP stack ignores this value if IPSECURITY is not specified on the IPCONFIG6 statement.

MONSYSPLEX | NOMONSYSPLEX
Specifies whether or not sysplex autonomics should monitor the interface's status.

NOMONSYSPLEX
Specifies that sysplex autonomics should not monitor the interfaces's status. This is the default value.

MONSYSPLEX
Specifies that sysplex autonomics should monitor the interface's status.

Restriction: The MONSYSPLEX attribute is not in effect unless the MONINTERFACE keyword is specified on the GLOBALCONFIG SYSPLEXMONITOR profile statement. The presence of dynamic routes over this interface is monitored if the DYNROUTE keyword is also specified on the GLOBALCONFIG SYSPLEXMONITOR profile statement.

DYNVLANREG | NODYNVLANREG
This parameter controls whether or not the VLAN ID for this interface is dynamically or statically registered with the physical switch on the LAN.

Restriction: This parameter is applicable only if a VLAN ID is specified on the statement.

Dynamic registration of VLAN IDs is handled by the OSA-Express feature and the physical switch on your LAN. Therefore, in order for the DYNVLANREG parameter to be effective, both must be at a level which provides the necessary hardware support for dynamic VLAN ID registration. After the interface is active, you can view the Netstat DEvlinks/**-d** report output to determine if your OSA-Express feature can support VLAN dynamic registration. This Netstat report also displays whether or not dynamic VLAN ID registration has been configured for the interface.

Rule: If you define both a LINK and INTERFACE statement for the same adapter, then the dynamic VLAN ID registration parameter value on the LINK statement must match the value of this same parameter on the corresponding INTERFACE statement. If you define an INTERFACE statement that contains a dynamic VLAN ID registration parameter value that conflicts with the same

parameter value for a previous INTERFACE statement for the same OSA-Express feature, then TCP/IP rejects the INTERFACE statement.

NODYNVLANREG
Specifies that if a VLAN ID is configured for this interface, it must be manually registered with the physical switches on the corresponding LAN. This is the default value. If this parameter is specified without a VLAN ID, then it is ignored.

DYNVLANREG
Specifies that if a VLAN ID is configured for this interface, it is dynamically registered with the physical switches on the corresponding LAN. If this parameter is specified without a VLAN ID, then warning message EZZ0056I is issued and the NODYNVLANREG setting is used instead.

VMAC *macaddr*
Specifies the virtual MAC address, which can be represented by 12 hexadecimal characters. The OSA-Express device uses this address rather than the physical MAC address of the device for all IPv6 packets to and from this TCP/IP stack. For CHPIDTYPE OSD, using a virtual MAC address is optional. For CHPIDTYPE OSX, using a virtual MAC address is required, so the VMAC parameter is the default.

The *macaddr* value is optional for CHPIDTYPE OSD and cannot be specified for CHPIDTYPE OSX. If the *macaddr* value is not coded, then the OSA-Express device generates a virtual MAC address. If the *macaddr* is coded, it must be defined as a locally administered individual MAC address. This means the MAC address must have bit 6 (the universal or local flag U bit) of the first byte set to 1 and bit 7 (the group or individual flag G bit) of the first byte set to 0. The second hexadecimal character must be 2, 6, A or E. The bit positions within the 12 hexadecimal characters are indicated as follows:

```
|               1|1               3|3               4|
|0              5|6               1|2               7|
+----------------+----------------+----------------+
|xxxxxxUGxxxxxxxx|xxxxxxxxxxxxxxxx|xxxxxxxxxxxxxxxx|
+----------------+----------------+----------------+
```

Rules:

- The same virtual MAC address generated by the OSA-Express device at interface activation remains in effect for this OSA-Express for this TCP/IP stack, even if the interface is stopped or becomes inoperative (INOPs). A new Virtual MAC address is generated only if the INTERFACE statement is deleted and redefined, or if the TCP/IP stack is recycled.
- The NONROUTER, PRIROUTER, and SECROUTER parameters are ignored for an OSA-Express interface if the VMAC parameter is configured on the INTERFACE statement.

Guideline: Unless the virtual MAC address representing this OSA-Express device must remain the same even after TCP/IP termination and restart, configure VMAC without a *macaddr* value and allow the OSA-Express device to generate it. This guarantees that the VMAC address is unique from all other physical burned-in MAC addresses and from all other VMAC addresses generated by any OSA-Express feature.

ROUTEALL
Specifies that all IP traffic destined to the virtual MAC is forwarded by the

OSA-Express device to the TCP/IP stack. This is the default value. See the router information in z/OS Communications Server: IP Configuration Guide for more details.

ROUTELCL
This specifies that only traffic destined to the virtual MAC and whose destination IP address is registered with the OSA-Express device by this TCP/IP stack is forwarded by the OSA-Express. See the router information in z/OS Communications Server: IP Configuration Guide for more details.

SMCR | NOSMCR
Specifies whether this interface can be used with Shared Memory Communications over Remote Direct Memory Access (SMC-R) for external data network communications.

NOSMCR
Specifies that this interface cannot be used for new TCP connections with SMC-R for external data network communications.

SMCR
Specifies that this interface can be used for new TCP connections with SMC-R for external data network communications. This is the default setting.

Rules:

- SMCR and NOSCMR are valid with CHPIDTYPE OSD definitions only.
- SMCR has no effect unless at least one Peripheral Component Interconnect Express (PCIe) function ID (PFID) value is specified by using the PFID subparameter of the SMCR parameter on the GLOBALCONFIG statement.

Guideline: If you enable Multipath and equal-cost interfaces are associated with different IP subnets, enabling SMC for some of, but not all, the interfaces can cause unpredictable SMC usage. You must specify either SMCR or NOSMCR on all equal-cost interfaces.

SMCD | NOSMCD
Specifies whether this interface can be used with Shared Memory Communications - Direct Memory Access (SMC-D).

NOSMCD
Specifies that this interface cannot be used for new TCP connections with SMC-D.

SMCD
Specifies that this interface can be used for new TCP connections with SMC-D. This is the default setting.

Rule: SMCD and NOSMCD are valid with CHPIDTYPE OSD definitions only.

Guideline: If you enable Multipath and equal-cost interfaces are associated with different IP subnets, enabling SMC for some of, but not all, the interfaces can cause unpredictable SMC usage. You must specify either SMCD or NOSMCD on all equal-cost interfaces.

OLM| NOOLM
An optional parameter indicating whether an OSA-Express adapter operates in optimized latency mode.

OLM Specifies that the OSA-Express adapter operates in optimized latency mode (OLM). Optimized latency mode optimizes interrupt processing

for both inbound and outbound data. Use this mode for workloads that have demanding latency requirements. Because this mode can provide significant increases of throughput, this mode is particularly suited for interactive, non-streaming workloads. For more information about OLM, see the optimized latency mode topic in z/OS Communications Server: IP Configuration Guide.

NOOLM
Specifies that the OSA-Express adapter should not operate in optimized latency mode. This is the default value.

Guidelines:

- Because of the operating characteristics of optimized latency mode, you might need to change configuration to direct traffic to particular OSA-Express write priority queues and to limit the number of concurrent users sharing an OSA-Express adapter configured for OLM. See the optimized latency mode topic in z/OS Communications Server: IP Configuration Guide. for more information.
- The optimized latency mode function targets a z/OS environment with high-volume interactive workloads. Although optimized latency mode can compensate for some mixing of workloads, an excessive amount of high-volume streaming workloads, such as bulk data or file transfer, can result in higher CPU consumption.

Restrictions:

- This function is limited to OSA-Express3 or later Ethernet features in QDIO mode that are running with an IBM System z10 or later. See the 2097 DEVICE Preventive Service Planning (PSP) bucket for more information.
- For an OSA-Express configured to use optimized latency mode, the stack ignores the configured or default INBPERF setting and uses the value DYNAMIC.

NOISOLATE | ISOLATE
Specifies whether packets should be directly routed between TCP/IP stacks that share the OSA adapter.

NOISOLATE
Route packets directly between TCP/IP stacks that share the OSA adapter. In this mode, if the next hop address was registered by another stack that is sharing the OSA, then OSA-Express routes the packet directly to the sharing stack without putting the packet on the external LAN.

ISOLATE
Prevent OSA-Express from routing packets directly to another TCP/IP stack that is sharing the OSA adapter. In this mode, OSA-Express discards any packets when the next hop address was registered by another stack that is sharing the OSA adapter. In this mode, packets can flow between two stacks that share the OSA adapter only by first going through a router on the LAN. For more details, see OSA-Express connection isolation information in z/OS Communications Server: IP Configuration Guide.

Tips:

- If you isolate an INTERFACE, that action might have an adverse effect on latency.
- You can selectively apply OSA-Express connection isolation to individual virtual LANs.

- OSA-Express requires that both stacks sharing the port be non-isolated for direct routing to occur. Therefore, for traffic between two stacks sharing the OSA adapter, as long as at least one of the stacks is isolated, connection isolation is in effect for traffic in both directions between these stacks.

Restriction: This function is limited to OSA-Express2 or later Ethernet features in QDIO mode and running at least an IBM System z9 Enterprise Class (EC) or z9 Business Class (BC). See the 2094, 2096, 2097, or 2098 DEVICE Preventive Service Planning (PSP) and the 2096DEVICE Preventive Service Planning (PSP) buckets for more information.

TEMPPREFIX

TEMPPREFIX specifies the set of prefixes for which temporary IPv6 addresses can be generated. A temporary IPv6 address is generated when a router advertisement containing a prefix is processed and the prefix is included in one of the prefixes in the temporary prefix list. For example, if TEMPPREFIX 2001:0db8:58cd::/48 is specified for an interface, a temporary address is generated for advertised prefix 2001:0db8:58cd:0001/64; however, a temporary address is not generated for advertised prefix 2001:0db8:5555:0001/64.

ALL Generate temporary addresses for all prefixes that are learned over this interface by way of router advertisements. ALL is the default.

NONE
No IPv6 temporary addresses are generated for this interface.

prefix/prefix_length
The digits (in colon-hexadecimal format) before the slash (/) represent the prefix. The *prefix_length* value represents the length of the prefix, in bits. Valid values for *prefix_length* are in the range 1 - 64.

Rules:

- Temporary addresses are generated only on an interface that is enabled for stateless address autoconfiguration.
- Temporary addresses are generated only when the TEMPADDRS keyword is specified on the IPCONFIG6 statement.

Requirement: You must specify the job name of an application in the SRCIP statement block with a value of TEMPADDRS to cause a temporary IPv6 address to be preferred over a public IPv6 address as the source IP address for the application; otherwise, the default source address selection algorithm prefers public IPv6 addresses over temporary addresses. For more information, see the information about the default source address selection algorithm in z/OS Communications Server: IPv6 Network and Application Design Guide.

Steps for modifying

See Summary of INTERFACE statements for modification information.

Examples

```
INTERFACE OSAQDIO26 ; OSA QDIO (Fast Ethernet)
DEFINE IPAQENET6
PORTNAME OSAQDIO2
SOURCEVIPAINT VIPAV6
IPADDR 2001:0DB8:1:9:67:115:66     ; (Global Address)
```

Usage notes

Restriction: For each interface, the PRIROUTER and SECROUTER attributes can be in effect for only one TCP/IP instance within a central processor complex (CPC). If PRIROUTER is specified for an IPAQENET6 interface, but the IPv6 primary router attribute is already in effect on another TCP/IP instance for the same OSA-Express, then TCP/IP issues a warning message during interface activation and ignores the PRIROUTER parameter. Therefore, only one TCP/IP instance can be the primary router for the OSA-Express. Depending on the level of OSA-Express being started, either only one or multiple TCP/IP instances can be allowed to have SECROUTER specified. If OSA-Express allows only one secondary router, any TCP/IP instance subsequently starting that interface with SECROUTER receives a warning message during START processing for the interface. If OSA-Express allows multiple secondary routers, then OSA-Express can select any TCP/IP instance which specifies SECROUTER as the secondary router. There is no requirement that the same TCP/IP instance be specified PRIROUTER or SECROUTER for all OSA-Express adapters attached to the CPC.

Rule: To configure a single OSA port for both IPv4 and IPv6 traffic, consider the following conditions:

- If you use DEVICE/LINK/HOME for the IPv4 definition and INTERFACE for the IPv6 definition, the PORTNAME value on the INTERFACE statement must match the device_name on the DEVICE statement. This combination shares a single DATAPATH device.
- If you use INTERFACE for both IPv4 and IPv6 definitions, the PORTNAME value on the IPv4 INTERFACE statement must match the PORTNAME value on the IPv6 INTERFACE statement. This combination results in separate DATAPATH devices.

Related topics

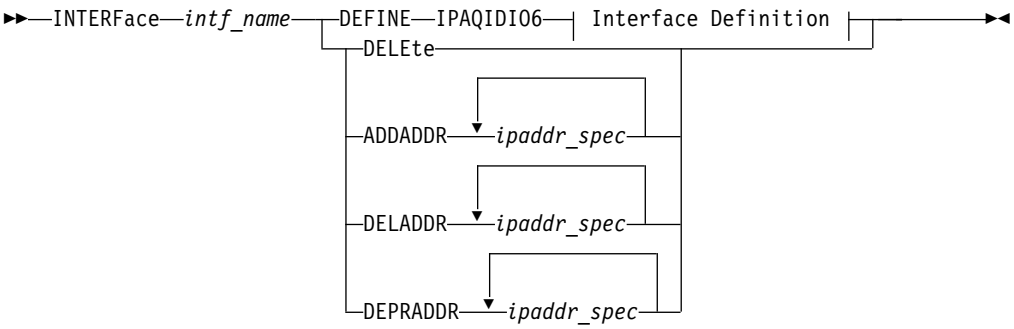
- BEGINROUTES statement
- DEVICE and LINK - MPCIPA OSA-Express QDIO devices statement
- “GLOBALCONFIG statement” on page 55
- “INTERFACE - IPAQENET OSA-Express QDIO interfaces statement” on page 79
- START statement
- STOP statement

INTERFACE - IPAQIDIO6 HiperSockets interfaces statement

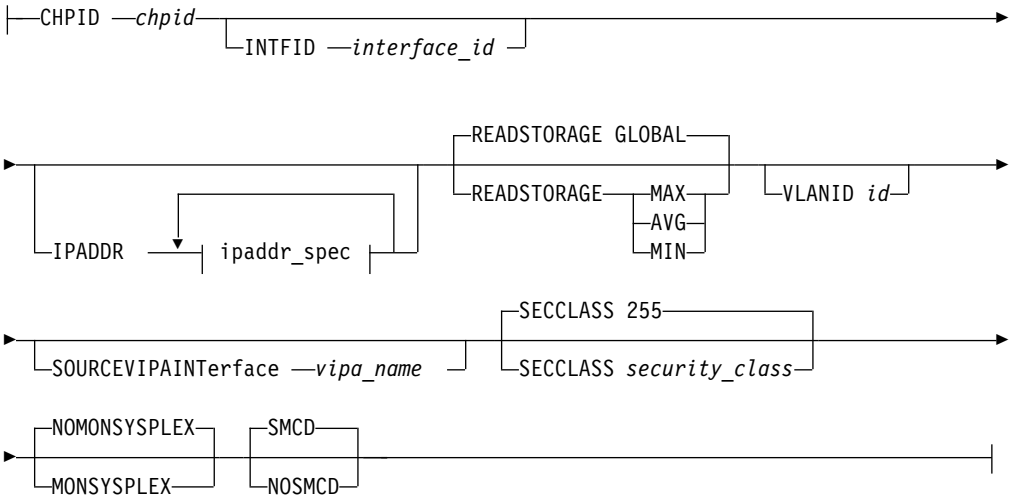
Use the INTERFACE statement for IPAQIDIO6 to configure IPv6 HiperSockets connectivity. Use the CHPID parameter to specify the value of the desired IQD CHPID that was configured within HCD. HiperSockets interfaces do not require a corresponding TRLE definition. Instead, the TRLE is dynamically built when the interface is started.

Rule: Specify the required parameters in the order shown here. The Interface Definition parameters can be specified in any order.

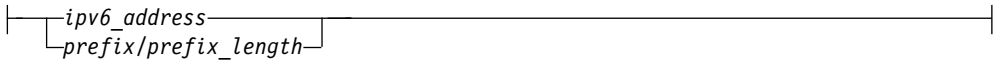
Syntax



Interface Definition:



ipaddr_spec:



Parameters

intf_name
The name of the interface. The maximum length is 16 characters.

Restriction: Do not specify the value PUBLICADDRS or TEMPADDRS for the interface name. The values PUBLICADDRS and TEMPADDRS are keywords on the SRCIP statement. These values are not recognized if they are specified as an IPv6 interface name on an SRCIP entry.

DEFINE
Specifies that this definition is to be added to the list of defined interfaces.

DELETE
Specifies that this definition is to be deleted from the list of defined interfaces. The *intf_name* must be the name of an interface previously defined by an INTERFACE statement. INTERFACE DELETE deletes all home IP addresses for the interface.

ADDADDR *ipaddr_spec*
Adds IP addresses to an existing INTERFACE definition (similar to an obeyfile

to update the home list) without having to delete and redefine the INTERFACE. The interface name (*intf_name*) coded with ADDADDR must be the name of an interface previously defined by an INTERFACE statement.

DELADDR *ipaddr_spec*
Deletes IP addresses from an existing INTERFACE definition. The DELADDR parameter is valid only for an IP address or prefix configured manually. The interface name (*intf_name*) coded with DELADDR must be the name of an interface previously defined by an INTERFACE statement. DELADDR is valid only in a VARY OBEYFILE profile.

Guideline: If you specify a prefix for DELADDR, then the only IP addresses affected are those defined by way of the same prefix specified on IPADDR or ADDADDR.

DEPRADDR *ipaddr_spec*
The DEPRADDR keyword allows you to deprecate an IP address. This can assist with site renumbering. DEPRADDR is valid only for an IP address or prefix configured manually. If you use DEPRADDR to deprecate an IP address, you can subsequently use ADDADDR again to make that IP address preferred. For DEPRADDR, the *interface_name* must be the name of an interface previously defined by an INTERFACE statement. DEPRADDR is valid only in a VARY OBEYFILE profile.

Guideline: If you specify a prefix for DEPRADDR, then the only IP addresses affected are those defined by way of the same prefix specified on IPADDR or ADDADDR.

IPADDR *ipaddr_spec*
The IPADDR parameter is optional, and is used to configure the interface's IPv6 addresses other than the link-local address (which is generated internally by TCP/IP).

Rule: Stateless Address Autoconfiguration does not apply to IPAQIDIO6 interfaces, you must manually configure any addresses (other than link-local) that are to be assigned to the IPAQIDIO6 interface.

If ADDADDR, DELADDR, DEPRADDR, or IPADDR is specified, then *ipaddr_spec* can be one of the following:

- ipv6_addr (A fully qualified IPv6 address in colon-hexadecimal format)
- prefix/prefix_length. Here, the digits (in colon-hexadecimal format) before the / represent the prefix. The prefix length represents the length of the prefix in bits. If a prefix length is coded, it must be equal to 64. When a prefix is specified, TCP/IP forms the IPv6 address by appending an interface ID to the specified prefix. The selected interface ID is either the value specified by way of the INTFID keyword, or the value returned by the device when the interface was started.

For information about the IPv6 address restrictions, see "INTERFACE - IPAQENET6 OSA-Express QDIO interfaces statement" on page 95.

IPAQIDIO6
Indicates that the interface is for HiperSockets IPv6.

INTFID *interface_id*
An optional 64-bit interface identifier in colon-hexadecimal format.

If specified, this interface ID is used to form the link-local address for the interface, and is also appended to any manually configured prefixes for the interface, to form complete IPv6 addresses on the interface.

If INTFID is not coded, TCP/IP builds the Interface ID using information returned from the HiperSockets device (during interface activation). The built Interface ID value is then used to form the link-local address. This value is also used to complete the formation of other IPv6 addresses on the interface, if you choose to configure only the prefix portion of the addresses (by way of IPADDR or ADDADDR).

For information about INTFID restrictions, see "INTERFACE - IPAQENET6 OSA-Express QDIO interfaces statement" on page 95.

SOURCEVIPAINTERFACE *vipa_name*
SOURCEVIPAINTERFACE is optional. Use this to specify which previously defined VIPA interface is to be used for SOURCEVIPA (when IPCONFIG6 SOURCEVIPA is in effect).

Tip: The use of the SOURCEVIPAINTERFACE parameter can be overridden. See the information about source IP address selection in z/OS Communications Server: IP Configuration Guide for the hierarchy of ways that the source IP address of an outbound packet is determined.The *vipa_name* is the interface name for a VIRTUAL6 interface. If the VIPA has multiple IP addresses, then the sourcevipa address for outbound packets is selected from among these addresses according to the default source address selection algorithm. For more information, see the default source address selection algorithm information in z/OS Communications Server: IPv6 Network and Application Design Guide.

Requirement: The VIRTUAL6 interface must be defined prior to specifying this INTERFACE statement to the TCP/IP stack. It must either already be defined or, the INTERFACE statement that defines it must precede this INTERFACE statement in the profile data set.

SECCLASS *security_class*
Use this parameter to associate a security class for IP filtering with this interface. In order for traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of 0. Filter rules can be specified in the TCP/IP profile or in an IP Security policy file read by the Policy Agent. Filter rules can include a security class specification on the IpService statement in an IP Security policy file or on the SECCLASS parameter on the IPSEC6RULE statement in the TCP/IP profile.

Valid security classes are identified as a number in the range 1 - 255. The default value is 255. For more information about security class values, see z/OS Communications Server: IP Configuration Guide.

Restriction: The TCP/IP stack ignores this value if IPSECURITY is not specified on the IPCONFIG6 statement.

MONSYSPLEX | NOMONSYSPLEX
Specifies whether or not sysplex autonomics should monitor the interface's status.

NOMONSYSPLEX
Specifies that sysplex autonomics should not monitor the interface's status. This is the default value.

MONSYSPLEX
Specifies that sysplex autonomics should monitor tinterface's status.

Restriction: The MONSYSPLEX attribute is not in effect unless the MONINTERFACE keyword is specified on the GLOBALCONFIG SYSPLEXMONITOR profile statement. The presence of dynamic routes

over the interface is monitored if the DYNROUTE keyword is also specified on the GLOBALCONFIG SYSPLEXMONITOR profile statement.

SMCD | NOSMCD
Specifies whether this interface can be used with Shared Memory Communications - Direct Memory Access (SMC-D).

NOSMCD
Specifies that this interface cannot be used for new TCP connections with SMC-D.

SMCD
Specifies that this interface can be used for new TCP connections with SMC-D. This is the default setting.

Guideline: If you enable Multipath and equal-cost interfaces are associated with different IP subnets, enabling SMC for some of, but not all, the interfaces can cause unpredictable SMC usage. You must specify either SMCD or NOSMCD on all equal-cost interfaces.

The following interface-specific values can be specified for IPAQIDIO6.

CHPID *chpid*
Use this parameter to specify the IQD CHPID for the HiperSockets interface. This value is a 2-character hexadecimal value (00x - FFx). The hexadecimal value specified on the CHPID parameter cannot be the same value that is used for the dynamic XCF HiperSockets interface. See IQDCHPID start option in the z/OS Communications Server: SNA Resource Definition Reference.

READSTORAGE
An optional parameter indicating the amount of fixed storage that z/OS CS should keep available for read processing for this interface. The IQDIOSTG VTAM start option allows you to specify a value which applies to all HiperSockets devices. You can use the READSTORAGE keyword to override the global IQDIOSTG value for this interface based on the inbound workload you expect over this interface on this stack. The valid values are:

GLOBAL
The amount of storage is determined by the IQDIOSTG VTAM start option. This is the default value.

MAX Use this value if you expect a heavy inbound workload over this interface.

AVG Use this value if you expect a medium inbound workload over this interface.

MIN Use this value if you expect a light inbound workload over this interface.

Tip: See the description of IQDIOSTG start option in the z/OS Communications Server: SNA Resource Definition Reference for details about exactly how much storage is allocated by z/OS Communications Server for each of these values.

Rules:

- If you define both a LINK and INTERFACE statement for the same device, then the READSTORAGE value on the LINK statement must match the READSTORAGE value on the corresponding INTERFACE statement.

- If you define an INTERFACE statement which contains a value for READSTORAGE which conflicts with the READSTORAGE value for a previous LINK statement for the same device, then TCP/IP rejects the INTERFACE statement.

VLANID *id*
An optional parameter followed by a decimal number indicating the virtual LAN identifier to be assigned to this HiperSockets interface. The valid range is 1 - 4094.

Restriction: HiperSockets allows a stack to specify only one VLAN ID if you define IPv4 connectivity by using DEVICE and LINK statements and also configure an IPv6 INTERFACE statement for the same CHPID. In this case, if you specify a different VLAN ID value on a LINK or INTERFACE definition for the same CHPID, the second statement is rejected.

Steps for modifying

See Summary of INTERFACE statements for modification information.

Examples

```
INTERFACE HIPERSOCK1 DEFINE IPAQIDIO6 CHPID FC
             IPADDR 12AB::7
```

Usage notes

Rule: To configure a single HiperSockets CHPID for both IPv4 and IPv6 traffic, consider the following conditions:

- If you use DEVICE/LINK/HOME for the IPv4 definition and INTERFACE for the IPv6 definition, the CHPID value on the INTERFACE statement must match the xx portion of the device_name (IUTIQDxx) on the DEVICE statement. This combination shares a single DATAPATH device.
- If you use INTERFACE for both IPv4 and IPv6 definition, the CHPID value on the IPv4 INTERFACE statement must match the CHPID value on the IPv6 INTERFACE statement. This combination results in separate DATAPATH devices.

Related topics

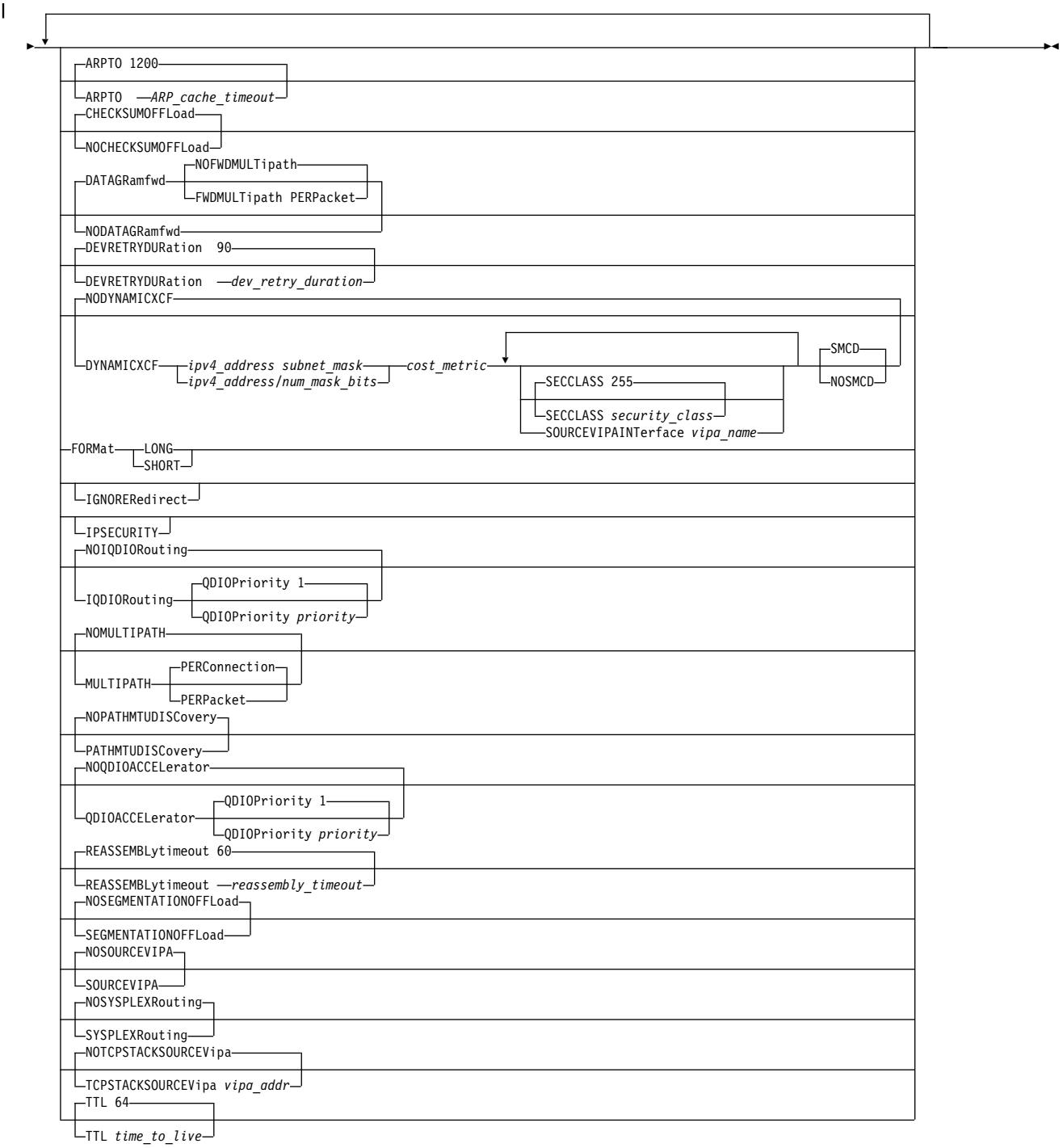
- BEGINROUTES statement
- DEVICE and LINK — MPCIPA HiperSockets devices statement
- “INTERFACE - IPAQIDIO HiperSockets interfaces statement” on page 91
- START statement
- STOP statement

IPCONFIG statement

Use the IPCONFIG statement to update the IPv4 IP layer of TCP/IP.

Syntax

Tip: Specify the parameters for this statement in any order.



Parameters

ARPTO *ARP_cache_timeout*

Use ARPTO to specify the number of seconds between creation or revalidation and deletion of ARP table entries. The default is 1200 seconds. An LCS ARP table entry is revalidated when another ARP packet is received from the same host specifying the same hardware address. The minimum value is 60, and the maximum value is 86400.

This parameter serves the same purpose as the ARPAGE statement, but the value specified on ARPAGE is in minutes while the value specified on the ARPTO parameter is in seconds.

Because ARP cache entries for MPCIPA and MPCOSA interfaces are not managed by the TCP/IP stack, they are not affected by the ARPTO statement. For more information about devices that support ARP Offload, see z/OS Communications Server: IP Configuration Guide.

CHECKSUMOFFLOAD | NOCHECKSUMOFFLOAD

Specifies whether the stack should offload inbound and outbound checksum processing (IP header, TCP, and UDP checksums) for IPv4 packets to OSA-Express features. The checksum offload support transfers the overhead of most checksum processing to QDIO-attached OSA-Express devices that support this function. Offloading checksum processing reduces CPU use and increases throughput. This parameter is ignored for OSA-Express features that do not support checksum offload.

See "Steps for modifying" on page 130 for information about changing this parameter while the TCP/IP stack is active. See Checksum offload in z/OS Communications Server: IP Configuration Guide for more information about the checksum offload support and for specific information about which packets can have checksum processing performed by the OSA-Express.

NOCHECKSUMOFFLOAD

Checksum processing is performed by the TCP/IP stack.

CHECKSUMOFFLOAD

Checksum processing is offloaded to the OSA-Express feature. This value is the default value.

DATAGRAMFWD | NODATAGRAMFWD

NODATAGRAMFWD

Disables the forwarding of IP packets that are received by, but not addressed to, the stack. This statement can be used for security or to ensure correct usage of limited resources. The NODATAGRAMFWD parameter is confirmed by the message:

```
EZZ0334I IP FORWARDING IS DISABLED
```

DATAGRAMFWD

Enables the forwarding of IP packets that are received by, but not addressed to, the stack. This is the default value.

Tip: The FWDMULTIPATH and NOFWDMULTIPATH keywords used with DATAGRAMFWD are independent of the MULTIPATH keyword on the IPCONFIG statement.

NOFWDMULTIPATH

When forwarding is in effect and there are multiple equal-cost routes to the destination and the NOFWDMULTIPATH parameter is specified, TCP/IP uses the first active route found for forwarding each IP packet. This is the default value. The DATAGRAMFWD NOFWDMULTIPATH parameter is confirmed by the message:

```
EZZ0641I IP FORWARDING NOFWDMULTIPATH SUPPORT IS ENABLED
```

FWDMULTIPATH PERPACKET

When forwarding is in effect and there are multiple equal-cost routes to the destination and the FWDMULTIPATH PERPACKET parameter is specified, TCP/IP selects a route for forwarding each

IP packet on an approximate round-robin basis from the multiple equal-cost routes. The selected route is used for routing that IP packet. Connection or connectionless-oriented IP packets using the same destination address do not always use the same route, but they do use all possible active routes to that destination host. All IP packets for a given association with a destination host are spread across the multiple equal-cost routes. The DATAGRAMFWD FWDMULTIPATH PERPACKET parameter is confirmed by the message:

```
EZZ0641I IP FORWARDING FWDMULTIPATH PERPACKET SUPPORT IS ENABLED
```

Guideline: If the TCP/IP stack is also configured to be a sysplex distributor (see VIPADYNAMIC statement summary for more information), datagrams destined to a sysplex-distributed dynamic VIPA are forwarded to stacks, whether or not forwarding is enabled.

DEVRETRYDURATION *dev_retry_duration*

Specifies the duration (in seconds) of the retry period for a failed device or interface. TCP/IP performs reactivation attempts at 30 second intervals during this retry period. The default for DEVRETRYDURATION is 90 seconds. A specification of 0 generates an infinite recovery period, which means reactivation attempts are performed until the device or interface is either successfully reactivated or manually stopped (by way of the VARY TCPIP,,STOP command, or the VARY TCPIP,,OBEYFILE command with a data set containing the STOP profile statement). The maximum specifiable value is 4294967295.

Guideline: The default 90–seconds retry duration is sufficient for transparent recovery following many types of device or channel errors. However, certain ESCON-attached routers cannot complete a microcode load in 90 seconds and installations might want to increase the DEVRETRYDURATION to automatically recover the device following these longer outages. On the other hand, installations running extensive automation built upon SNMP status and alerts can choose to code a small (nonzero) value in DEVRETRYDURATION, such that device recovery is deferred to external automation software, rather than a function of TCP/IP. For IPv4 interfaces that are defined with DEVICE and LINK statements, see also the AUTORESTART parameter in Overview of DEVICE and LINK statements. For IPv6 interfaces and IPv4 interfaces that are defined with the INTERFACE statement, the autorestart function is always active.

DYNAMICXCF | NODYNAMICXCF

Indicates XCF support status.

NODYNAMICXCF

Indicates XCF dynamic support is not enabled. The NODYNAMICXCF parameter is confirmed by the message:

```
EZZ0624I DYNAMIC XCF DEFINITIONS ARE DISABLED
```

NODYNAMICXCF is the default value.

DYNAMICXCF

Indicates that dynamic XCF support is enabled for IPv4.

When DYNAMICXCF is coded in the profile, the purpose is to generate dynamic XCF interfaces, if possible. When TCP/IP is active, but ISTLSXCF is not active, dynamic creation is deferred. Later, when a TCP/IP command such as VARY TCPIP,,OBEYFILE or VARY TCPIP,,START is executed, triggering profile processing, the stack again

checks to see if ISTLSXCF is active. If ISTLSXCF is active at that time, then the dynamic XCF interfaces are generated.

Dynamic XCF definitions are not generated if there is a DEVICE and LINK definition with the same device or link name that dynamic XCF would generate, or if there is an INTERFACE definition with the same interface name that dynamic XCF would generate.

Activation of dynamic XCF interfaces is delayed if VTAM is not up or if OMPROUTE is not up and DELAYJOIN is coded on the GLOBALCONFIG SYSPLEXMONITOR statement. For more information about connectivity problems in a sysplex, see z/OS Communications Server: IP Configuration Guide.

When using dynamic XCF for Sysplex configuration, make sure that XCFINIT=YES or XCFINIT=DEFINE is coded in the VTAM start options, or if XCFINIT=NO was specified, ensure that a VARY ACTIVATE command is issued for the ISTLSXCF major node. This ensures that XCF connections between TCP stacks on different VTAM nodes in the sysplex can be established. See z/OS Communications Server: SNA Resource Definition Reference for directions to code the XCFINIT VTAM start option. The DISPLAY NET,VTAMOPTS command can be used to determine the XCFINIT setting.

cost_metric
: Specifies the interface-level metric for the cost of use for the DYNAMICXCF interface. The *cost_metric* value is an integer in the range 0 - 14. If using OMPROUTE, the *cost_metric* value is overridden with a corresponding OMPROUTE interface parameter value that can be coded or set to the default value (Cost0= on OSPF_INTERFACE or In_Metric= on RIP_INTERFACE).

ipv4_address
: The IP address to be used as the home address for all dynamically generated XCF, Same Host, and HiperSockets interfaces. A multicast address is not accepted in this case.

subnet_mask
: Specifies the interface-level subnet mask for the DYNAMICXCF interface. If using OMPROUTE, the *subnet_mask* value is overridden with a corresponding OMPROUTE interface parameter value that can be coded or set to the default value.

/num_mask_bits
: It is an integer value in the range 1 - 32 that represents the number of leftmost significant bits for the address mask.

SECCLASS *security_class*
: Use this parameter to associate a security class for IP filtering with each dynamic XCF interface. In order for traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of 0. Filter rules can be specified in the TCP/IP profile or in an IP Security policy file read by the Policy Agent. Filter rules can include a security class specification on the IpService statement in an IP Security policy file or on the SECCLASS parameter on the IPSEC statement in the TCP/IP profile.

Valid security classes are identified as a number in the range 1 - 255. The default value is 255. For more information about security class values, see z/OS Communications Server: IP Configuration Guide.

This value is used only when IPSECURITY is specified on the IPCONFIG statement.

SOURCEVIPAINTERFACE *vipa_name*
The SOURCEVIPAINTERFACE parameter is optional. This parameter specifies which static VIPA interface is to be used as the source IP address when IPCONFIG SOURCEVIPA is specified and outbound packets are sent over the dynamically generated XCF, Same Host, or HiperSockets interfaces. The *vipa_name* value is the interface name for a VIRTUAL interface. The maximum length is 16 characters.

The use of the SOURCEVIPAINTERFACE parameter can be overridden. See Source IP address selection in z/OS Communications Server: IP Configuration Guide for the hierarchy of ways that the source IP address of an outbound packet is determined.

SMCD | NOSMCD
Specifies whether the dynamically generated XCF HiperSockets interface can be used for new TCP connections with Shared Memory Communications - Direct Memory Access (SMC-D).

SMCD
Specifies that the dynamically generated XCF HiperSockets interface can be used for new TCP connections with SMC-D. This is the default setting.

NOSMCD
Specifies that the dynamically generated XCF HiperSockets interface cannot be used for new TCP connections with SMC-D.

Rule: SMCD has no effect unless a nonzero subnet mask is configured on the DYNAMICXCF statement.

Requirement: The VTAM ISTLSXCF major node must be active for XCF dynamics to work, except for the following scenarios:

- Multiple TCP/IP stacks on the same MVS image; a dynamic samehost definition is generated whether ISTLSXCF is active or not.
- HiperSockets is configured and enabled across multiple z/OS systems that are in the same sysplex and the same CEC; a dynamic IUTIQDIO link is created whether ISTLSXCF is active or not.

For information about activating the ISTLSXCF major node, see z/OS Communications Server: SNA Resource Definition Reference.

Restriction: A mix of static and dynamic IPv4 and IPv6 definitions for a device are not allowed. For example, if a static IUTSAMEH IPv4 interface is defined, then the IPv6 dynamic definition for IUTSAMEH is not created. If a static IUTSAMEH IPv6 interface is defined, then the IPv4 dynamic definition for IUTSAMEH is not created. The same logic is also applied for XCF interfaces; a mix of static and dynamic IPv4 and IPv6 definitions is not allowed for an XCF interface.

Guidelines:

1. Dynamic XCF can be enabled even in a single system sysplex. HiperSockets can be used between LPARs on the same central processor complex (CPC) even when MVS images in those LPARs are not defined to be part of the same sysplex. HiperSockets can also be used between LPARs even when some of those other LPARs are running Linux, as long as all of the stacks connecting to HiperSockets and needing to exchange IP packets with each other define IP addresses that are all in the same subnet (as defined by the dynamic XCF IP address and subnet mask in the IPCONFIG DYNAMICXCF profile statement).
2. If the DYNAMICXCF parameter is added (using a VARY TCPIP,,OBEYFILE command data set) after the TCP/IP stack and OMPROUTE are active, the DYNAMICXCF link should be configured to OMPROUTE prior to issuing the VARY TCPIP,,OBEYFILE command. If you do not do this, the network mask is used as the subnet mask for the interface.

For more details about the use of DYNAMICXCF, see the DYNAMICXCF information in z/OS Communications Server: IP Configuration Guide. The DYNAMICXCF parameter is confirmed by the message:

```
EZZ0624I DYNAMIC XCF DEFINITIONS ARE ENABLED
```

FORMAT

The FORMAT keyword is optional, and there is no default.

The FORMAT keyword is meaningful only for stacks that are not enabled for IPv6. It controls the format of the command output. If FORMAT SHORT is specified and the stack is enabled for IPv6, then an error message is displayed. If the stack is not enabled for IPv6 and the user specified LONG format, the command output is displayed as if it could contain IPv6 addresses. If the stack is not enabled for IPv6 and the user specified SHORT format or did not specify the FORMAT keyword, then the command output is displayed as if it could contain only IPv4 addresses and not the longer IPv6 addresses.

If the stack is enabled for IPv6, then specifying the FORMAT keyword does not make any difference to the command format

IGNOREREDIRECT

Causes TCP/IP to ignore ICMP Redirect packets. The IGNOREREDIRECT parameter is confirmed by the message:

```
EZZ0335I ICMP WILL IGNORE REDIRECTS
```

If you are using OMPROUTE and you have IPv4 interfaces configured to OMPROUTE and this option is not specified, IGNOREREDIRECT is enabled automatically.

If you are using intrusion detection services (IDS) policy to detect and discard ICMP Redirects and this option is not specified, ICMP Redirects are discarded anyway while the policy is active.

If this option is not specified, and an ICMP redirect is received for a destination for which there is a HOST route in the routing table, then the original route is deleted and replaced by the redirect. This applies to all routes, including static routes.

IPSECURITY

Activates IPv4 IP filtering and IPv4 IPSec tunnel support.

Requirements:

- Use this parameter so that the stack can function with the Communications Server IKE daemon, and for the stack to receive IPv4 IPSec policy information such as IP filter rules from the policy agent.
- Use this parameter so that the stack can receive defensive filters from the Defense Manager daemon (DMD).

The IPSECURITY parameter is confirmed by the message:

```
EZZ0753I IPV4 SECURITY SUPPORT IS ENABLED
```

Restriction: IPSec functions can be activated only at initial activation of TCP/IP.

IQDIOROUTING | NOIQDIOROUTING

NOIQDIOROUTING

Specifies that inbound packets that are to be forwarded by this TCP/IP stack should not be routed directly between a HiperSockets device and an OSA-Express device in QDIO mode. These packets are processed and routed by this TCP/IP stack.

NOIQDIOROUTING is the default value. If NOIQDIOROUTING is explicitly specified, then the stack confirms that direct routing is disabled with the following message:

```
EZZ0688I IQDIO ROUTING IS DISABLED
```

IQDIOROUTING

Specifies that inbound packets that are to be forwarded by this TCP/IP stack are eligible to be routed directly between a HiperSockets device and an OSA-Express device in QDIO mode without needing to be sent to this TCP/IP stack for forwarding. This type of routing over a HiperSockets device (iQDIO) is called HiperSockets Accelerator. If specified, HiperSockets Accelerator routes are created dynamically as this TCP/IP stack learns of destination IP addresses that can be routed to or from HiperSockets links without needing to be forwarded to this TCP/IP stack. HiperSockets Accelerator support cannot be enabled if the IPSECURITY parameter or the NODATAGRAMFWD parameter is specified. Use of the IQDIOROUTING parameter is confirmed by the following message:

```
EZZ0688I IQDIO ROUTING IS ENABLED
```

If HiperSockets Accelerator support cannot be enabled, message EZZ0689I is issued with the reason. This message is also issued if IQDIOROUTING is specified in the data set that is used with the VARY TCPIP,,OBEYFILE command, if TCP/IP was activated with NOIQDIOROUTING and NOQDIOACCELERATOR on the initial profile.

Rule: This parameter is ignored if QDIOACCELERATOR is specified.

Restrictions:

- HiperSockets Accelerator support cannot be enabled during VARY TCPIP,,OBEYFILE command processing unless either IQDIOROUTING or QDIOACCELERATOR was specified on the IPCONFIG statement in the initial profile.
- HiperSockets Accelerator does not accelerate packets either from or to interfaces configured with optimized latency mode. For more information about optimized latency mode, see Optimized latency mode in z/OS Communications Server: IP Configuration Guide.

- You cannot enable HiperSockets accelerator support if you specify the NODATAGRAMFWD parameter.
- You cannot enable HiperSockets accelerator support if you specify the IPSECURITY parameter.

QDIOPRIORITY priority
If traffic is being routed by way of HiperSockets Accelerator, the data is sent using the priority level specified by priority. *priority* values are in the range 1 - 4. The default is to send data using priority level 1. See the OSA-Express documentation in z/OS Communications Server: SNA Network Implementation Guide.

QDIOACCELERATOR | NOQDIOACCELERATOR

NOQDIOACCELERATOR
Specifies that inbound packets that are to be forwarded by this TCP/IP stack should not be routed directly between any of the following combinations of interface types:

- A HiperSockets interface and an OSA-Express QDIO interface
- Two OSA-Express QDIO interfaces
- Two HiperSockets interfaces

These packets are processed and routed by this TCP/IP stack.

NOQDIOACCELERATOR is the default value. If NOQDIOACCELERATOR is explicitly specified, the stack confirms this type of routing with the message:

```
EZZ0817I QDIO ACCELERATOR IS DISABLED
```

QDIOACCELERATOR
Specifies that inbound packets that are to be forwarded by this TCP/IP stack are eligible to be routed directly between any of the following combinations of interface types:

- A HiperSockets interface and an OSA-Express QDIO interface
- Two OSA-Express QDIO interfaces
- Two HiperSockets interfaces

These packets do not need to be sent to this TCP/IP stack for forwarding. This also applies to packets that would be forwarded by the Sysplex Distributor. This type of routing is called QDIO Accelerator. See the information about QDIO Accelerator in z/OS Communications Server: IP Configuration Guide for more details on this function.

Use of the QDIOACCELERATOR parameter is confirmed by one of the following messages:

```
EZZ0817I QDIO ACCELERATOR IS ENABLED
EZZ0819I QDIO ACCELERATOR IS ENABLED FOR SYSPLEX DISTRIBUTOR ONLY
EZD2020A QDIO ACCELERATOR IS ENABLED ONLY FOR SYSPLEX DISTRIBUTOR BECAUSE OF TCPIP PROFILE FILTER RULES
EZD2021A QDIO ACCELERATOR IS ENABLED ONLY FOR SYSPLEX DISTRIBUTOR BECAUSE OF POLICY FILTER RULES
EZD2022A QDIO ACCELERATOR IS ENABLED ONLY FOR SYSPLEX DISTRIBUTOR BECAUSE OF DEFENSIVE FILTER RULES
EZD2023I QDIO ACCELERATOR IS ENABLED WITH CURRENTLY INSTALLED IP FILTER RULES
```

You receive the following message with the appropriate reason if QDIO Accelerator support cannot be enabled. You also receive this message if QDIOACCELERATOR is specified in the data set used with the VARY TCPIP,,OBEYFILE command, if TCP/IP was activated with NOIQDIOROUTING and NOQDIOACCELERATOR on the initial profile.

```
EZZ0818I CANNOT ENABLE QDIO ACCELERATOR - reason
```

Rule: IQDIOROUTING is ignored if QDIOACCELERATOR is specified.

Restrictions:

- If you specify the NODATAGRAMFWD parameter, then QDIO Accelerator applies only to packets that are forwarded by the Sysplex Distributor.
- If you specify the IPSECURITY parameter, TCP/IP monitors your IP filter rules and defensive filter rules that apply to routed traffic. Depending on your filter configuration, QDIO Accelerator might be restricted to only packets that are forwarded by the Sysplex Distributor. For more information about QDIO Accelerator and IPSECURITY, see Search orders used in the native MVS environment in z/OS Communications Server: IP Configuration Guide.
- QDIO Accelerator support cannot be enabled during VARY TCPIP,,OBEYFILE command processing unless either QDIOACCELERATOR or IQDIOROUTING was specified on the IPCONFIG statement in the initial profile.
- QDIO Accelerator does not accelerate packets either from or to interfaces configured with optimized latency mode. For more information about optimized latency mode, see Optimized latency mode in z/OS Communications Server: IP Configuration Guide.

QDIOPRIORITY *priority*

Specifies that traffic routed by QDIO Accelerator to an OSA-Express QDIO interface be sent using the priority level specified by the *priority* value. The priority level can be in range 1 - 4. The default is to send data using priority level 1. See the OSA-Express information in the z/OS Communications Server: SNA Network Implementation Guide.

MULTIPATH | NOMULTIPATH

NOMULTIPATH

Disables the multipath routing selection algorithm for outbound IP traffic. If there are multiple equal-cost routes to a destination and NOMULTIPATH is specified, TCP/IP uses the first active route found to send each IP packet. The NOMULTIPATH parameter is confirmed by the message:

```
EZZ0615I MULTIPATH SUPPORT IS DISABLED
```

This is the default value.

Rule: The NOMULTIPATH parameter applies to outbound IP traffic that is routed by using the main route table. This parameter applies also to outbound IP traffic that is routed by using a policy-based route table if the Multipath UseGlobal parameter is specified on the RouteTable statement that defines the policy-based route table. See RouteTable statement for more information.

MULTIPATH

Enables the multipath routing selection algorithm for outbound IP traffic. In general, multipath routing provides the routing distribution necessary to balance the network utilization of outbound packets by load splitting. Multipath routing requires multiple equal-cost routes that are either defined statically or added dynamically by routing protocols (except for RIP, which does not provide multipath routing). If MULTIPATH is specified without any subparameters, the default is

PERCONNECTION. The MULTIPATH parameter has no effect if there are no multipath routes in the TCP/IP configuration.

Guideline: In some cases, it might appear data is not being equally distributed among each of the equal-cost interfaces. This depends upon the characteristics of the application that is sending or receiving data. For example, when `osnmp walk` is issued, the application initially sends data using a source IP address of INADDR_ANY. Subsequently, when the application receives a response, all future sends use the source IP address of the interface where data was just received. The result is that all data is sent out on a single interface, independent of any multipath setting.

Rules:

- The MULTIPATH parameter and its subparameters apply to outbound IP traffic that is routed by using the main route table. This parameter and its subparameters apply also to outbound IP traffic that is routed by using a policy-based route table if the Multipath UseGlobal parameter is specified on the RouteTable statement that defines the policy-based route table. See RouteTable statement for more information.
- The multipath routing selection algorithm is applied and can be specified separately for each route table. Specify the algorithm for the main route table by using the MULTIPATH parameter on the IPCONFIG statement. Specify the algorithm for policy-based route tables in the policy definition for each table. See RouteTable statement for more information.

Note: The IPCONFIG MULTIPATH|NOMULTIPATH configuration option affects Enterprise Extender (EE) traffic when MULTPATH=TCPVALUE is coded. For information about multipath for EE see z/OS Communications Server: SNA Network Implementation Guide. For information about the MULTPATH start option, see z/OS Communications Server: SNA Resource Definition Reference.

PERCONNECTION

After a round-robin route is selected, connection or connectionless oriented IP packets using the same association always use the same route, as long as that route is active. The MULTIPATH PERCONNECTION parameter is confirmed by the message:

```
EZZ0632I MULTIPATH PERCONNECTION SUPPORT IS ENABLED
```

For more information about EE load balancing and standard logic for a UDP application, see z/OS Communications Server: SNA Network Implementation Guide.

PERPACKET

Connection or connectionless oriented IP packets using the same source and destination address pair do not always use the same route, but do use all possible active routes to that destination host. The MULTIPATH PERPACKET parameter is confirmed by the message:

```
EZZ0632I MULTIPATH PERPACKET SUPPORT IS ENABLED
```

Restrictions:

- Use this option only as an attempt to improve aggregate throughput of IP traffic over multipath routes and for routes for which potentially high CPU consumption in reassembly of out-of-order packets at the receiving end is not an issue. Performance varies according to network configurations used.
- The MULTIPATH PERPACKET parameter cannot be specified if IP security is configured. If both are specified, the following messages are displayed, and multipath routing is disabled:

  ```
  EZZ0763I CANNOT ENABLE IPV4 MULTIPATH PERPACKET SUPPORT WHEN
           IPV4 SECURITY IS ENABLED
  EZZ0615I MULTIPATH SUPPORT IS DISABLED
  ```

- IP traffic on RSVP-based routes cannot use this option. Instead, the PERCONNECTION option is used for these routes.
- Fragmented and packed IP datagrams cannot use this option. These datagrams are being sent over one selected route to the intended destination.

PATHMTUDISCOVERY | NOPATHMTUDISCOVERY

NOPATHMTUDISCOVERY
Indicates that TCP/IP is not to provide path MTU (PMTU) discovery support. This is the default value. The NOPATHMTUDISCOVERY parameter is confirmed by the message:

```
EZZ0623I PATH MTU DISCOVERY SUPPORT IS DISABLED
```

PATHMTUDISCOVERY
Indicates that TCP/IP is to dynamically discover the PMTU, which is the smallest MTU of all the hops in the path. Use this parameter to prevent fragmentation of datagrams. The PATHMTUDISCOVERY parameter is confirmed by the message:

```
EZZ0623I PATH MTU DISCOVERY SUPPORT IS ENABLED
```

Requirement: PATHMTUDISCOVERY uses ICMP fragmentation-needed errors to detect the PMTU for a path. If you use PATHMTUDISCOVERY, you must permit ICMP errors to flow at all hosts along the path of a connection. PATHMTUDISCOVERY does not function if a firewall blocks ICMP errors.

For a policy-based route table, the IgnorePathMtuUpdate parameter on the Policy Agent RouteTable statement can be used to prevent the path MTU value from being updated for routes in the table. See the information about the IgnorePathMtuUpdate parameter in RouteTable statement for information about determining when you should prevent the path MTU value from being updated for a policy-based route table.

REASSEMBLYTIMEOUT *reassembly_timeout*
The amount of time (in seconds) allowed to receive all parts of a fragmented packet before the fragments received are discarded. The minimum value is 1, the maximum value is 240, and the default is 60.

SEGMENTATIONOFFLOAD | NOSEGMENTATIONOFFLOAD
Specifies whether the stack should offload TCP segmentation for IPv4 packets to OSA-Express features. The TCP segmentation offload support transfers the overhead of segmenting outbound data into individual TCP packets to QDIO-attached OSA-Express devices that support this function. Offloading

segmentation of streaming-type workloads reduces CPU use and increases throughput. This parameter is ignored for OSA-Express features that do not support segmentation offload. This value overrides the SEGMENTATIONOFFLOAD or NOSEGMENTATIONOFFLOAD parameter specified on the GLOBALCONFIG statement.

See the steps for modifying topic for information about changing this parameter while the TCP/IP stack is active. See TCP segmentation offload in z/OS Communications Server: IP Configuration Guide for more information about TCP segmentation offload support.

NOSEGMENTATIONOFFLOAD
TCP segmentation is performed by the TCP/IP stack. This value is the default value.

SEGMENTATIONOFFLOAD
TCP segmentation is offloaded to the OSA-Express feature.

SOURCEVIPA | NOSOURCEVIPA

NOSOURCEVIPA
Specifies that TCP/IP is not requested to use the corresponding virtual IP address in the HOME list as the source IP address for outbound datagrams. The NOSOURCEVIPA parameter is confirmed by the message:

```
EZZ0351I SOURCEVIPA SUPPORT IS DISABLED.
```

NOSOURCEVIPA is the default value.

SOURCEVIPA
Requests that TCP/IP use the TCPSTACKSOURCEVIPA address (if specified) or the corresponding virtual IP address in the HOME list as the source IP address for outbound datagrams that do not have an explicit source address. If the outgoing interface was defined with the INTERFACE statement, TCP/IP uses the VIPA specified on the SOURCEVIPAINTERFACE parameter of the INTERFACE statement instead of the HOME list. You must specify the TCPSTACKSOURCEVIPA parameter, update the HOME statement, or use the SOURCEVIPAINTERFACE parameter of the INTERFACE statement for the SOURCEVIPA parameter to take effect. For more information about how the order of the HOME list impacts source VIPA selection, see HOME statement. This parameter has no effect on OMPROUTE RIP packets used by RIP services or OSPF packets used by OSPF services. The SOURCEVIPA parameter is confirmed by the following message:

```
EZZ0351I SOURCEVIPA SUPPORT IS ENABLED
```

Tip: You can override the SOURCEVIPA or TCPSTACKSOURCEVIPA values. See the information about source IP address selection in z/OS Communications Server: IP Configuration Guide for the hierarchy of ways that the source IP address of an outbound packet is determined.

SYSPLEXROUTING | NOSYSPLEXROUTING

NOSYSPLEXRouting
Specifies that this TCP/IP host is not part of an MVS sysplex domain. Use of the NOSYSPLEXROUTING parameter is confirmed by the message:

```
EZZ0350I SYSPLEX ROUTING SUPPORT IS DISABLED
```

NOSYSPLEXROUTING is the default value.

SYSPLEXRouting
Specifies that this TCP/IP host is part of an MVS sysplex domain. The SYSPLEXROUTING parameter is confirmed by the message:

```
EZZ0350I SYSPLEX ROUTING SUPPORT IS ENABLED
```

TCPSTACKSOURCEVIPA | NOTCPSTACKSOURCEVIPA

NOTCPSTACKSOURCEVIPA
Specifies that TCP/IP does not use a stack-level IP address as the source address for outbound TCP connections. The source IP address is governed by the IPCONFIG SOURCEVIPA setting.

TCPSTACKSOURCEVIPA *vipa_addr*
The IPv4 address (*vipa_addr*) is used as the source IP address for outbound TCP connections if SOURCEVIPA has been enabled. The *vipa_addr* value must be a static VIPA or an active dynamic VIPA (DVIPA).

If SOURCEVIPA has not been enabled, TCPSTACKSOURCEVIPA is ignored, and the following message is issued:

```
EZZ0706I TCPSTACKSOURCEVIPA IS IGNORED - SOURCEVIPA IS NOT ENABLED
```

Restriction: At the time of an outbound TCP request, the TCPSTACKSOURCEVIPA address must be a static VIPA or active dynamic VIPA, or it is not used for the source IP address.

Tips:

- After it is set, TCPSTACKSOURCEVIPA is not disabled until a profile explicitly adds NOTCPSTACKSOURCEVIPA to the IPCONFIG statement.
- If you specify the same distributed DVIPA interface for TCPSTACKSOURCEVIPA on multiple target stacks, you also should specify SYSPLEXPORTS on the VIPADISTRIBUTE statement. Otherwise connections might be disrupted because identical connections could be created from more than one stack.
- Carefully consider the following condition when determining the interface to use for TCPSTACKSOURCEVIPA. A dynamic VIPA that becomes inactive because it moves to another TCP/IP stack, or that is deleted because the application that caused its creation (in the case of a VIPARANGE created address) causes its deletion, is no longer a valid interface for TCPSTACKSOURCEVIPA.
- The use of TCPSTACKSOURCEVIPA can be overridden. See the information about source IP address selection in z/OS Communications Server: IP Configuration Guide for the hierarchy of ways that the source IP address of an outbound packet is determined.
- TCPSTACKSOURCEVIPA is not used when an outbound TCP request is connecting to an IP address that is active in the Home list.

TTL *time_to_live*
Number of hops that packets originating from this host can travel before reaching the destination. If the destination is more hops away, the packet never reaches the destination. The minimum value is 1, the maximum value is 255, and the default is 64.

Steps for modifying

To modify most parameters for the IPCONFIG statement, you must respecify the statement with the new parameters. Additional actions are required to modify the following parameters:

CHECKSUMOFFLOAD | NOCHECKSUMOFFLOAD
If the CHECKSUMOFFLOAD or NOCHECKSUMOFFLOAD parameter is changed with the VARY TCPIP,,OBEYFILE command, the new value does not affect any active OSA-Express QDIO interfaces. For this change to affect an active OSA-Express QDIO interface, the interface must be stopped and restarted.

DYNAMICXCF
If dynamic XCF definitions have been enabled but a later VARY TCPIP,,OBEYFILE command contains NODYNAMICXCF, only future dynamic definitions and connectivity are affected. Existing definitions and connectivity are not affected.

After support is enabled, none of the parameters specified on the IPCONFIG DYNAMICXCF statement can be changed with a VARY TCPIP,,OBEYFILE command. You must first stop the TCP/IP stack, apply changes, and then restart the TCP/IP stack.

IPSECURITY
z/OS IPSec functions cannot be activated using VARY TCPIP,,OBEYFILE on an active TCP/IP stack. To activate z/OS IPSec, halt all traffic on the designated TCP/IP stack, stop the stack, modify the TCP profile to include IPCONFIG IPSECURITY, and restart the stack.

IQDIOROUTING
If HiperSockets Accelerator is active then:

- You can disable HiperSockets Accelerator by issuing the VARY TCPIP,,OBEYFILE command and specifying IPCONFIG NOIQDIOROUTING.
- You can activate QDIO Accelerator by issuing the VARY TCPIP,,OBEYFILE command and specifying IPCONFIG NOIQDIOROUTING QDIOACCELERATOR.

If HiperSockets Accelerator and QDIO Accelerator are not active and you want to enable HiperSockets Accelerator, enable HiperSockets Accelerator by issuing the VARY TCPIP,,OBEYFILE command and specifying IPCONFIG IQDIOROUTING (if either IQDIOROUTING or QDIOACCELERATOR was specified in the initial profile); otherwise, stop the stack, modify the profile to include IPCONFIG IQDIOROUTING and restart the stack.

NODATAGRAMFWD
If HiperSockets Accelerator is enabled and IP forwarding is subsequently disabled by issuing a VARY TCPIP,,OBEYFILE with NODATAGRAMFWD specified, HiperSockets Accelerator is also disabled. If HiperSockets Accelerator is disabled, and IPCONFIG IQDIOROUTING is subsequently specified on a VARY TCPIP,,OBEYFILE command for an active TCP/IP stack where IP Forwarding is disabled, HiperSockets Accelerator remains disabled.

If QDIO Accelerator is enabled and IP Forwarding is subsequently disabled using NODATAGRAMFWD in a VARY TCPIP,,OBEYFILE command data set, QDIO Accelerator remains enabled but only for Sysplex Distributor

forwarding. If QDIO Accelerator is disabled and IPCONFIG QDIOACCELERATOR is subsequently specified on a VARY TCPIP,,OBEYFILE command for an active TCP/IP stack on which IP forwarding is disabled, QDIO Accelerator is enabled for Sysplex Distributor forwarding only.

QDIOACCELERATOR
If QDIO Accelerator is active:

- You can disable QDIO Accelerator by issuing the VARY TCPIP,,OBEYFILE command and specifying IPCONFIG NOQDIOACCELERATOR.
- You can activate HiperSockets Accelerator by issuing the VARY TCPIP,,OBEYFILE command and specifying IPCONFIG NOQDIOACCELERATOR IQDIOROUTING.

If QDIO Accelerator and HiperSockets Accelerator are not active and you want to enable QDIO Accelerator, enable QDIO Accelerator by issuing the VARY TCPIP,,OBEYFILE command and specifying IPCONFIG QDIOACCELERATOR (if either IQDIOROUTING or QDIOACCELERATOR was specified in the initial profile); otherwise, stop the stack, modify the profile to include IPCONFIG QDIOACCELERATOR and restart the stack.

MULTIPATH
If you modify the multipath routing type (PERCONNECTION to PERPACKET, or vice versa), the new parameter takes effect only for new connections created after the modification is done, and existing connections use whatever the value was when the connection was established. If you enable multipath routing when it was previously disabled, existing connections are not affected; multipath routing is applied only to new connections.

SEGMENTATIONOFFLOAD | NOSEGMENTATIONOFFLOAD
If the SEGMENTATIONOFFLOAD or NOSEGMENTATIONOFFLOAD parameter is changed with the VARY TCPIP,,OBEYFILE command, the new value does not affect any active OSA-Express QDIO interfaces. For this change to affect an active OSA-Express QDIO interface, the interface must be stopped and restarted.

Examples

```
IPCONFIG ARPTO 2400 NODATAGR
DYNAMICXCF 9.9.9.9 255.255.255.0 15
```

This example shows an IPCONFIG statement that does the following tasks:

- Causes ARP table entries to be deleted 2400 seconds after creation or revalidation
- Disables IP forwarding
- Enables dynamic XCF support and indicates that 9.9.9.9 is the IP address to be used for HOME statements for all dynamically generated XCF, Same Host, and HiperSockets links. These links have an interface-level subnet mask of 255.255.255.0 and a metric of 15.

Usage notes

- If the stack is enabled for IPv6 and the user specified LONG format, the command output is displayed in IPv6 format.

- The FORMAT keyword is meaningful only for stacks that are not enabled for IPv6. It controls the format of the command output. If FORMAT SHORT is specified and the stack is enabled for IPv6, then the following error message is displayed:

  ```
  EZZ0687I FORMAT SHORT IGNORED - IPV6 SUPPORT IS ENABLED
  ```

- If you do not include any configuration data in the OMPROUTE configuration file for the XCF links, OMPROUTE does not communicate a routing protocol (OSPF or RIP) over the interfaces. OMPROUTE includes (in the data sent to other routers) information relative to the XCF links as long as Send_Static_Routes=YES is configured for RIP Interfaces and AS_Boundary_Routing(Import_Static_Routes=YES) is configured for OSPF.

  Rule: If you want to communicate the OSPF or RIP protocol over a subset of the XCF links, you must configure the appropriate links in the OMPROUTE configuration file using the OSPF_Interface or RIP_Interface statements. Doing this enables OMPROUTE to communicate to other routers not only the information relative to the XCF links, but also information relative to resources on the other side of the host at the opposite end of the XCF links.

  To configure the appropriate links, you can explicitly configure each XCF link as either an OSPF or RIP interface (including those that might become active in the future). Alternatively, you can use the wildcard configuration capability of OMPROUTE to configure your XCF links.

  To use the wildcard configuration, use a wildcard address (for example, 9.67.100.*) on the OSPF_Interface or RIP_Interface statement instead of an explicit address. In this way, any interface address falling within that wildcard range (9.67.100.1, 9.67.100.2, and so on) is configured using the parameters specified on the wildcard definition statement.

  When adding links, XCF or otherwise, to both OMPROUTE and TCP/IP, it is necessary to add them to OMPROUTE before adding them to TCP/IP for proper routing protocol configuration.

Related topics

- "GLOBALCONFIG statement" on page 55
- "IPCONFIG6 statement"
- SRCIP statement

IPCONFIG6 statement

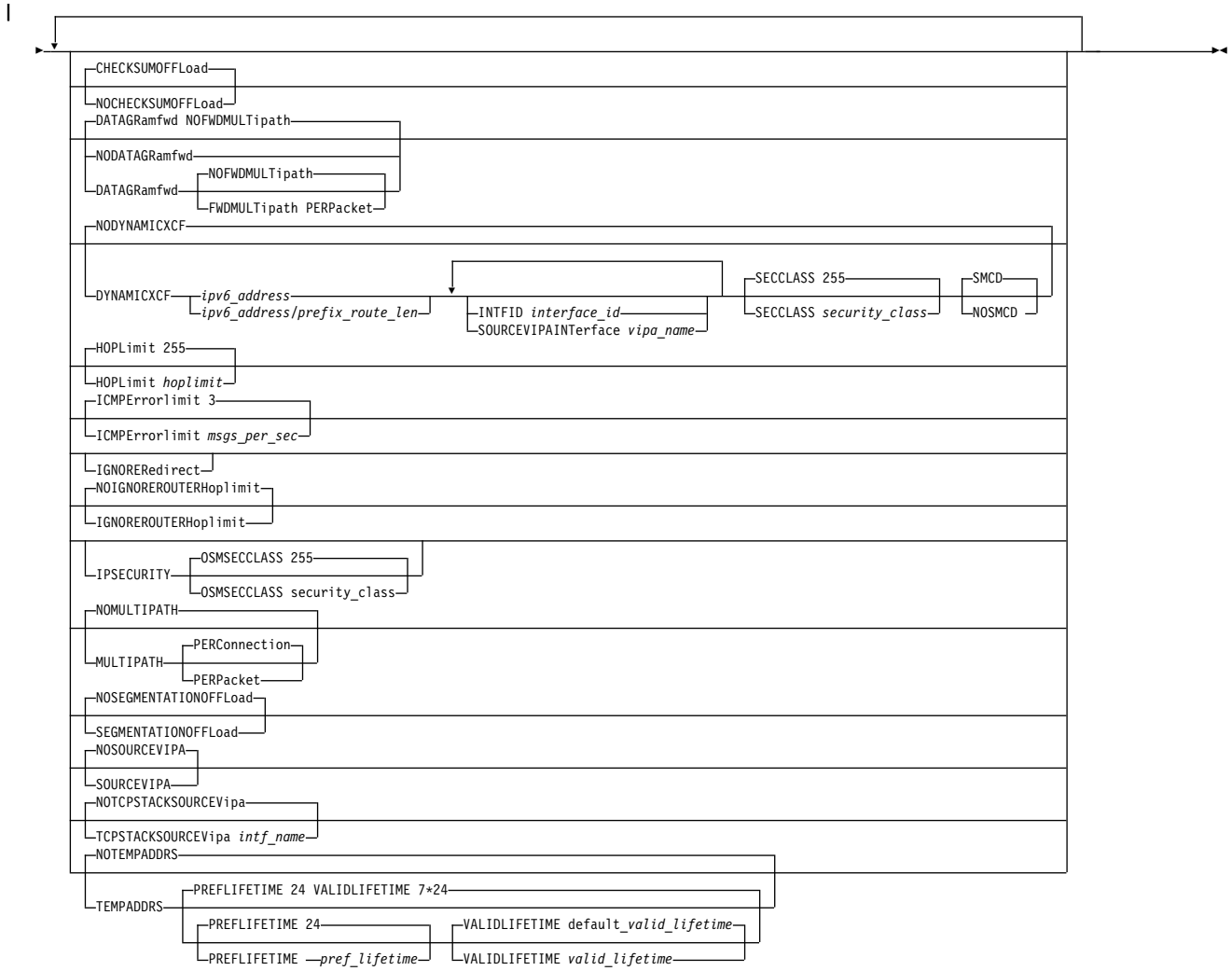
Use the IPCONFIG6 statement to update the IP layer of TCP/IP with information that pertains to IPv6.

If the stack is not configured for IPv6 and IPCONFIG6 is specified, the following error message is generated, and TCP/IP startup processing continues.

```
EZZ0695I IPCONFIG6 NOT VALID - IPV6 SUPPORT IS NOT ENABLED
```

Syntax

Tip: Specify the parameters for this statement in any order.



Parameters

CHECKSUMOFFLOAD | NOCHECKSUMOFFLOAD

Specifies whether the stack should offload inbound and outbound checksum processing (TCP and UDP checksums) for IPv6 packets to OSA-Express features. The checksum offload support transfers the overhead of most checksum processing to QDIO-attached OSA-Express devices that support this function. Offloading checksum processing reduces CPU use and increases throughput. This parameter is ignored for OSA-Express features that do not support IPv6 checksum offload.

See "Steps for modifying" on page 143 for information about changing this parameter while the TCP/IP stack is active. See Checksum offload in z/OS Communications Server: IP Configuration Guide for more information about the checksum offload support and for specific information about which packets can have checksum processing performed by the OSA-Express.

NOCHECKSUMOFFLOAD

Checksum processing is performed by the TCP/IP stack.

CHECKSUMOFFLOAD

Checksum processing is offloaded to the OSA-Express feature. This value is the default value.

DATAGRAMFWD | NODATAGRAMFWD

NODATAGRAMFWD

Disables the forwarding of IP packets that are received by, but not addressed to, the stack. This statement can be used for security or to ensure correct usage of limited resources. The NODATAGRAMFWD parameter is confirmed by the message:

```
EZZ0699I IPV6 FORWARDING IS DISABLED
```

If the TCP/IP stack is also configured to be a sysplex distributor (see VIPADYNAMIC statement summary for more information), datagrams destined to a sysplex-distributed dynamic VIPA are forwarded to stacks, whether or not forwarding is enabled.

DATAGRAMFWD

Enables the forwarding of IP packets that are received by, but not addressed to, the stack. This is the default value.

NOFWDMULTIPATH

When forwarding is in effect and there are multiple equal-cost routes to the destination and the NOFWDMULTIPATH parameter is specified, TCP/IP uses the first active route found for forwarding each IP packet. This is the default value. The DATAGRAMFWD NOFWDMULTIPATH parameter is confirmed by the message:

```
EZZ0700I IPV6 FORWARDING NOFWDMULTIPATH SUPPORT IS ENABLED
```

FWDMULTIPATH PERPACKET

When forwarding is in effect and there are multiple equal-cost routes to the destination and the FWDMULTIPATH PERPACKET parameter is specified, TCP/IP selects a route for forwarding each IP packet on an approximate round-robin basis from the multiple equal-cost routes. Connection or connectionless-oriented IP packets using the same destination address do not always use the same route, but they do use all possible active routes to that destination host. All IP packets for a given association with a destination host are spread across the multiple equal-cost routes. The DATAGRAMFWD FWDMULTIPATH PERPACKET parameter is confirmed by the message:

```
EZZ0700I IPV6 FORWARDING FWDMULTIPATH PERPACKET SUPPORT IS ENABLED
```

DYNAMICXCF | NODYNAMICXCF

NODYNAMICXCF

Indicates XCF dynamic support is not enabled for IPv6 on this TCP/IP. The NODYNAMICXCF parameter for IPCONFIG6 is confirmed by the message:

```
EZZ0739I IPV6 DYNAMIC XCF DEFINITIONS ARE DISABLED
```

DYNAMICXCF

Indicates that dynamic XCF support is enabled for IPv6.

When DYNAMICXCF is coded in the profile, the purpose is to generate those dynamic XCF devices or interfaces, if possible. When TCP/IP is up, but ISTLSXCF is not active, dynamic creation is deferred. Later, when a TCP/IP command such as VARY TCPIP,,OBEYFILE or VARY TCPIP,,START is executed, triggering profile processing, the stack again checks to see if ISTLSXCF is active. If ISTLSXCF is active at that time, then the dynamic XCF devices and interfaces are generated.

Dynamic XCF definitions are not generated if there is a DEVICE or INTERFACE definition with the same device or interface name that dynamic XCF would generate.

Activation of dynamic XCF links is delayed if VTAM is not up or if OMPROUTE is not up and DELAYJOIN is coded on the GLOBALCONFIG SYSPLEXMONITOR statement. For more information about connectivity problems in a sysplex, see z/OS Communications Server: IP Configuration Guide.

When using dynamic XCF for sysplex configuration, make sure that XCFINIT=YES or XCFINIT=DEFINE is coded in the VTAM start options, or if XCFINIT=NO was specified, ensure that a VARY ACTIVATE command is issued for the ISTLSXCF major node. This ensures that XCF connections between TCP stacks on different VTAM nodes in the sysplex can be established. See z/OS Communications Server: SNA Resource Definition Reference for directions for coding the XCFINIT VTAM start option. The DISPLAY NET,VTAMOPTS command can be used to determine the XCFINIT setting.

The VTAM ISTLSXCF major node must be active for XCF dynamics to work, except for the following two scenarios:

- Multiple TCP/IP stacks on the same MVS image; a dynamic samehost definition is generated, whether ISTLSXCF is active or not.
- HiperSockets is configured and enabled across multiple z/OS systems that are in the same sysplex and the same CEC; a dynamic IUTIQDIO link is created, whether ISTLSXCF is active or not.

For information about activating the ISTLSXCF major node, see z/OS Communications Server: SNA Resource Definition Reference.

Dynamic XCF can be enabled even in a single system sysplex. HiperSockets can be used between LPARs on the same central processor complex (CPC) even when MVS images in those LPARs are not defined to be part of the same sysplex. HiperSockets can also be used between LPARs even when some of those other LPARs are running Linux, as long as all of the stacks connecting to HiperSockets and needing to exchange IP packets with each other define IP addresses that are all in the same subnet (as defined by the dynamic XCF IP address and subnet mask in the IPCONFIG6 DYNAMICXCF profile statement).

A mix of static and dynamic IPv4 and IPv6 definitions for a device are not allowed. For example, if a static IUTSAMEH IPv4 device/link is defined, then the IPv6 dynamic definition for IUTSAMEH is not created. If a static IUTSAMEH IPv6 interface is defined, then the IPv4 dynamic definition for IUTSAMEH is not created. The same logic is also applied for XCF links; a mix of static and dynamic IPv4 and IPv6 definitions is not allowed for an XCF link.

ipv6_address
The fully qualified IPv6 address that is used for all dynamically generated XCF, Same Host, and HiperSockets interfaces.

See Restrictions on IPv6 addresses configured in the TCP/IP profile for a list of restrictions that must be observed when specifying this parameter.

prefix_route_len
The length of the routing prefix (an integer value in the range 1 -

128). If specified, and if DYNAMICXCF generates a HiperSockets interface definition, TCP/IP creates a prefix route over the HiperSockets interface using the number of bits specified in *prefix_route_len* of the *ipv6_address*. Therefore, you can configure other stacks outside the sysplex for the same IQD CHPID using IP addresses with the same prefix such that this stack automatically has a route to these other stacks over the HiperSockets interface generated by DYNAMICXCF. If *prefix_route_len* is not specified, then TCP/IP does not create a prefix route over the HiperSockets interface. For interfaces other than HiperSockets which are generated from DYNAMICXCF, the *prefix_route_len* value has no meaning.

Guideline: Configure a *prefix_route_len* to simplify connectivity if you use HiperSockets on the same IQD CHPID for stacks outside the sysplex or if you configure VIPAROUTE statements.

INTFID *interface_id*
An optional 64-bit interface identifier in colon-hexadecimal format. IPv6 address shorthand notation (for example, the use of :: to indicate multiple groups of 16 bits of zeros) is not allowed when specifying the interface ID. If specified, this interface ID is used to form the link-local address for the interface.

If INTFID is not coded, TCP/IP generates a random value to be used to form the link-local address.

See "INTERFACE - IPAQENET6 OSA-Express QDIO interfaces statement" on page 95 for an explanation of restrictions that must be observed when manually specifying the INTFID parameter.

SOURCEVIPAINTERFACE *vipa_name*
The SOURCEVIPAINTERFACE parameter is optional. This parameter specifies which static VIPA interface is to be used as the source IP address when IPCONFIG6 SOURCEVIPA is specified and outbound packets are sent over the dynamically generated XCF or Same Host interfaces. The *vipa_name* value is the interface name for a VIRTUAL6 interface. If the VIPA has multiple IP addresses, then the source VIPA address for outbound packets is selected from among these addresses according to the default source address selection algorithm. The maximum length is 16 characters. For more information, see the default source address selection algorithm information in z/OS Communications Server: IPv6 Network and Application Design Guide.

The use of the SOURCEVIPAINTERFACE parameter can be overridden. See the information about source IP address selection in z/OS Communications Server: IP Configuration Guide for the hierarchy of ways that the source IP address of an outbound packet is determined.

SECCLASS *security_class*
Use this parameter to associate a security class for IP filtering with each IPv6 dynamic XCF interface. In order for traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of 0. Filter rules can be specified in the TCP/IP profile or in an IP Security policy file read by the Policy Agent. Filter rules can include a security class

specification on the IpService statement in an IP Security policy file or on the SECCLASS parameter on the IPSEC6RULE statement in the TCP/IP profile.

Valid security classes are identified as a number in the range 1 - 255. The default value is 255. For more information about security class values, see z/OS Communications Server: IP Configuration Guide.

Restriction: This value is used only when IPSECURITY is specified on the IPCONFIG6 statement.

SMCD | NOSMCD
Specifies whether the dynamically generated XCF HiperSockets interface can be used for new TCP connections with Shared Memory Communications - Direct Memory Access (SMC-D).

SMCD
Specifies that the dynamically generated XCF HiperSockets interface can be used for new TCP connections with SMC-D. This is the default setting.

NOSMCD
Specifies that the dynamically generated XCF HiperSockets interface cannot be used for new TCP connections with SMC-D.

For more details about the use of DYNAMICXCF, see the DYNAMICXCF information in z/OS Communications Server: IP Configuration Guide. The DYNAMICXCF parameter is confirmed by the message:

```
EZZ0739I IPV6 DYNAMIC XCF DEFINITIONS ARE ENABLED
```

HOPLIMIT *hoplimit*
Number of hops a packet originating at this host can travel enroute to the destination. If the destination is more hops away, the packet never reaches the destination. The valid range is between 1 - 255. The default is 255.

ICMPERRORLIMIT *msgs_per_sec*
This parameter controls the rate at which ICMP error messages can be sent to a particular IPv6 destination address. The number specified is messages per second. The default is 3 messages per second, and the valid range is 1 - 20 messages per second. A token bucket algorithm is used to allow bursts of ICMP errors while limiting the long-term rate.

IGNOREREDIRECT
Causes TCP/IP to ignore ICMPv6 Redirect packets. The IGNOREREDIRECT parameter is confirmed by the message:

```
EZZ0701I ICMPV6 REDIRECTS WILL BE IGNORED
```

If you are using OMPROUTE, and IPv6 interfaces are configured to OMPROUTE, and this option is not specified, IGNOREREDIRECT is enabled automatically. If you are using intrusion detection services (IDS) policy to detect and discard ICMPv6 redirect packets and this option is not specified, ICMPv6 redirect packets are discarded while the policy is active.

IGNOREROUTERHOPLIMIT | NOIGNOREROUTERHOPLIMIT

NOIGNOREROUTERHOPLIMIT
NOIGNOREROUTERHOPLIMIT causes TCP/IP to not ignore a hop limit value received in a router advertisement from a router over an

IPAQENET6 interface. This results in the configured global hop limit value being overridden by the router advertisement value for all routes using the interface on which the router advertisement was received. This is the default value. The NOIGNOREROUTERHOPLIMIT parameter is confirmed by the message:

```
EZZ0720I ROUTER ADVERTISEMENT HOP LIMIT VALUES WILL NOT BE IGNORED
```

IGNOREROUTERHOPLIMIT

Although you can configure a global hop limit value for the stack (by way of IPCONFIG6 HOPLIMIT), your stack might receive a different hop limit value in a router advertisement from a router, over an IPAQENET6 interface. This results in the configured global hop limit value being overridden by the router advertisement value for all routes using the interface on which the router advertisement was received. IGNOREROUTERHOPLIMIT gives you a way to prevent this, ensuring that your configured value is always used. The IGNOREROUTERHOPLIMIT parameter is confirmed by the message:

```
EZZ0719I ROUTER ADVERTISEMENT HOP LIMIT VALUES WILL BE IGNORED
```

IPSECURITY

Activates IPv6 IP filtering and IPv6 IPSec tunnel support. This parameter requires the IPSECURITY parameter to be configured for IPv4 on the IPCONFIG statement.

Requirements:

- Use this parameter so that the stack can function with the Communications Server IKE daemon and to enable the stack to receive IPv6 IPSec policy information, such as IP filter rules from the policy agent.
- Use this parameter so that the stack can receive IPv6 defensive filters from the Defense Manager daemon (DMD).

The IPSECURITY parameter is confirmed by the message:

```
EZZ0786I IPV6 SECURITY SUPPORT IS ENABLED
```

Restriction: IPSec functions can be activated only at initial activation of TCP/IP.

OSMSECCLASS *security_class*

Use this parameter to associate a security class for IP filtering with each OSM interface. In order for traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of 0. Filter rules can be specified in the TCP/IP profile or in an IP Security policy file read by the Policy Agent. Filter rules can include a security class specification on the IpService statement in an IP Security policy file or on the SECCLASS parameter on the IPSEC6RULE statement in the TCP/IP profile. For more information about OSM interfaces, see the TCP/IP in an intraensemble network section in z/OS Communications Server: IP Configuration Guide.

Valid security classes are identified as a number in the range 1 - 255. The default value is 255. For more information about security class values, see z/OS Communications Server: IP Configuration Guide.

MULTIPATH | NOMULTIPATH

NOMULTIPATH

Disables the multipath routing selection algorithm for outbound IP traffic. If there are multiple equal-cost routes to a destination and

NOMULTIPATH is specified, TCP/IP uses the first active route found to send each IP packet. The NOMULTIPATH parameter is confirmed by the message:

```
EZZ0703I IPV6 MULTIPATH SUPPORT IS DISABLED
```

NOMULTIPATH is the default value.

Rule: The NOMULTIPATH parameter applies to outbound IP traffic that is routed by using the main route table. This parameter applies also to outbound IP traffic that is routed by using a policy-based route table if the Multipath6 UseGlobal parameter is specified on the RouteTable statement that defines the policy-based route table. See RouteTable statement for more information.

MULTIPATH

Enables the multipath routing selection algorithm for outbound IP traffic. In general, multipath routing provides the routing distribution necessary to balance the network utilization of outbound packets by load splitting. Multipath routing requires the definition of multiple equal-cost routes that are either defined statically or added dynamically by routing protocols (except for RIP, which does not provide multipath routing). If MULTIPATH is specified without any subparameters, the default is PERCONNECTION. The MULTIPATH parameter has no effect if there are no multipath routes in the TCP/IP configuration.

Rules:

- The MULTIPATH parameter and its subparameters apply to outbound IP traffic that is routed by using the main route table. This parameter and its subparameters apply also to outbound IP traffic that is routed by using a policy-based route table if the Multipath6 UseGlobal parameter is specified on the RouteTable statement that defines the policy-based route table. See RouteTable statement for more information.
- The multipath routing selection algorithm is applied and can be specified separately for each route table. Specify the algorithm for the main route table using the MULTIPATH parameter on the IPCONFIG6 statement. Specify the algorithm for policy-based route tables in the policy definition for each table. See RouteTable statement for more information.

Note: The IPCONFIG6 MULTIPATH|NOMULTIPATH configuration option affects Enterprise Extender (EE) traffic when MULTPATH=TCPVALUE is coded. For information about multipath for EE, see z/OS Communications Server: SNA Network Implementation Guide. For information about the MULTPATH start option, see z/OS Communications Server: SNA Resource Definition Reference.

PERCONNECTION

If there are multiple equal-cost routes to a destination and MULTIPATH PERCONNECTION is specified, TCP/IP, upon first sending an IP packet to a given destination, selects a route on a round-robin basis from a multipath routing list to that destination host. The selected route is used to route IP packets for a given connection or connectionless oriented association to

that destination host. Connection or connectionless oriented IP packets using the same association always use the same route, as long as that route is active. The MULTIPATH PERCONNECTION parameter is confirmed by the message:

```
EZZ0704I IPV6 MULTIPATH PERCONNECTION SUPPORT IS ENABLED
```

PERPACKET

If there are multiple equal-cost routes to a destination, TCP/IP, upon sending an IP packet in that destination, selects a route on an approximate round-robin basis from a multipath routing list to that destination host. The selected route is used for routing that IP packet. Connection or connectionless oriented IP packets using the same source and destination address pair do not always use the same route, but do use all possible active routes to that destination host. All IP packets for a given association with a destination host are spread across the multiple equal-cost routes. The MULTIPATH PERPACKET parameter is confirmed by the message:

```
EZZ0704I IPV6 MULTIPATH PERPACKET SUPPORT IS ENABLED
```

Restriction: The MULTIPATH PERPACKET parameter cannot be enabled if the IPSECURITY parameter is specified. If both values are specified, the following messages are displayed, and multipath routing is disabled.

```
EZZ0792I CANNOT ENABLE IPV6 MULTIPATH PERPACKET SUPPORT WHEN
IPV6 SECURITY IS ENABLED
EZZ0703I IPV6 MULTIPATH SUPPORT IS DISABLED
```

SEGMENTATIONOFFLOAD | NOSEGMENTATIONOFFLOAD

Specifies whether the stack should offload TCP segmentation for IPv6 packets to OSA-Express features. The TCP segmentation offload support transfers the overhead of segmenting outbound data into individual TCP packets to QDIO-attached OSA-Express devices that support this function. Offloading segmentation of streaming-type workloads reduces CPU use and increases throughput. This parameter is ignored for OSA-Express features that do not support IPv6 segmentation offload.

See the steps for modifying topic for information about changing this parameter while the TCP/IP stack is active. See TCP segmentation offload in z/OS Communications Server: IP Configuration Guide for more information about the TCP segmentation offload support.

NOSEGMENTATIONOFFLOAD

TCP segmentation is performed by the TCP/IP stack. This value is the default value.

SEGMENTATIONOFFLOAD

TCP segmentation is offloaded to the OSA-Express feature.

SOURCEVIPA | NOSOURCEVIPA

NOSOURCEVIPA

Specifies that TCP/IP is not requested to use a VIPA address as the source IP address for outbound datagrams. The NOSOURCEVIPA parameter is confirmed by the message:

```
EZZ0702I IPV6 SOURCEVIPA SUPPORT IS DISABLED
```

NOSOURCEVIPA is the default value.

SOURCEVIPA

Requests that TCP/IP use a virtual IP address assigned to the TCPSTACKSOURCEVIPA interface (if TCPSTACKSOURCEVIPA is specified) or to the SOURCEVIPAINTERFACE interface as the source address for outbound datagrams that do not have an explicit source address. If multiple addresses are assigned to the TCPSTACKSOURCEVIPA interface or the SOURCEVIPAINTERFACE interface, the source address is selected from among these addresses according to the default source address selection algorithm. For more information, see the default source address selection algorithm information in z/OS Communications Server: IPv6 Network and Application Design Guide.

Requirement: You must specify the SOURCEVIPAINTERFACE keyword on the INTERFACE statement for each interface on which you want that SOURCEVIPA to take effect. The SOURCEVIPA parameter is confirmed by the message:

```
EZZ0702I IPV6 SOURCEVIPA SUPPORT IS ENABLED
```

Tip: The use of SOURCEVIPA or TCPSTACKSOURCEVIPA can be overridden. See the information about source IP address selection in z/OS Communications Server: IP Configuration Guide for the hierarchy of ways that the source IP address of an outbound packet is determined.

TCPSTACKSOURCEVIPA | NOTCPSTACKSOURCEVIPA

NOTCPSTACKSOURCEVIPA

Specifies that TCP/IP does not use a stack-level IPv6 address as the source address for outbound TCP connections. The source IP address is determined by the normal default selection.

TCPSTACKSOURCEVIPA *intf_name*

The name of a static VIPA or a dynamic VIPA interface. The maximum length is 16 characters.

If the interface has multiple IP addresses, then the sourcevipa address for outbound packets is selected from among these addresses according to the default source address selection algorithm. For more information, see the default source address selection algorithm information in z/OS Communications Server: IPv6 Network and Application Design Guide.

If SOURCEVIPA has not been enabled for IPCONFIG6, IPCONFIG6 TCPSTACKSOURCEVIPA is ignored and the following message is issued:

```
EZZ0760I IPV6 TCPSTACKSOURCEVIPA IS IGNORED - SOURCEVIPA IS NOT ENABLED
```

Tips:

- After it is set, TCPSTACKSOURCEVIPA is not disabled until a profile explicitly adds NOTCPSTACKSOURCEVIPA to the IPCONFIG6 statement.
- A dynamic VIPA that becomes inactive because it moves to another TCP/IP stack, or that is deleted because the application that caused its creation (in the case of a VIPARANGE statement created address) causes its deletion, is no longer a valid interface for the TCPSTACKSOURCEVIPA parameter.

- If you specify the same distributed DVIPA interface for TCPSTACKSOURCEVIPA on multiple target stacks, you also should specify SYSPLEXPORTS on the VIPADISTRIBUTE statement. Otherwise connections might be disrupted because identical connections could be created from more than one stack.
- Carefully consider the following when determining the interface to use for TCPSTACKSOURCEVIPA.
  - A dynamic VIPA that becomes inactive because it moves to another TCP/IP stack, or that is deleted because the application that caused its creation (in the case of a VIPARANGE statement created address) causes its deletion, is no longer a valid interface for TCPSTACKSOURCEVIPA.
  - A dynamic VIPA interface that is created by a VIPARANGE statement can have multiple dynamic VIPA addresses associated with it. The actual address chosen as the source IP for the outbound connection is not predictable or necessarily meaningful.
- The use of TCPSTACKSOURCEVIPA can be overridden. See the information about source IP address selection in z/OS Communications Server: IP Configuration Guide for the hierarchy of ways that the source IP address of an outbound packet is determined.

TEMPADDRS | NOTEMPADDRS

NOTEMPADDRS
Specifies that TCP/IP should not generate IPv6 temporary addresses. Use of the NOTEMPADDRS parameter is confirmed by the message:

```
EZZ0821I IPV6 TEMPORARY ADDRESS SUPPORT IS DISABLED
```

NOTEMPADDRS is the default value.

TEMPADDRS
Requests that TCP/IP generate IPv6 temporary addresses for IPAQENET6 OSA-Express QDIO interfaces for which stateless address autoconfiguration is enabled. Stateless address autoconfiguration is enabled for an interface if no address or prefix is specified with the IPADDR keyword. See the information about using IPv6 temporary addresses to address privacy concerns in the z/OS Communications Server: IPv6 Network and Application Design Guide.

Requirement: You must specify the job name of an application in the SRCIP statement block with a value of TEMPADDRS to cause a temporary IPv6 address to be preferred over a public IPv6 address as the source IP address for the application; otherwise, the default source address selection algorithm prefers public IPv6 addresses over temporary addresses. See the information about default source address selection in the z/OS Communications Server: IPv6 Network and Application Design Guide .

The TEMPADDRS parameter is confirmed by the message:

```
EZZ0816I IPV6 TEMPORARY ADDRESS SUPPORT IS ENABLED
```

PREFLIFETIME *pref_lifetime*
Preferred lifetime for temporary addresses specified in hours. At the expiration of the preferred lifetime, a new temporary address is generated and the existing address is deprecated. Valid values are in the range 1 - 720 hours (30 days). The default is 24 hours (1 day).

Results:

- A temporary address can be deprecated sooner than specified by the *pref_lifetime* value if the preferred lifetime of the prefix that is learned from a router advertisement is less than the *pref_lifetime*.
- A short preferred lifetime results in new temporary addresses being generated more quickly.

VALIDLIFETIME *valid_lifetime*
Valid lifetime for temporary addresses, specified in hours. At the expiration of the valid lifetime, the temporary address is deleted. Valid values are in the range 2 - 2160 hours (90 days). The default is 7 times the preferred lifetime, not to exceed a maximum value of 90 days.

Rules:

- *valid_lifetime* value must be greater than *pref_lifetime* value.
- If PREFLIFETIME is not explicitly configured, the *valid_lifetime* value must be greater than the default value for *pref_lifetime*.

Results:

- A temporary address can be deleted sooner than specified by the *valid_lifetime* value if the valid lifetime of the prefix that is learned from a router advertisement is less than *valid_lifetime*.
- A short valid lifetime results in deprecated temporary addresses being deleted more quickly.

Guideline: Do not specify a small *pref_lifetime* value with a large *valid_lifetime* value. A large number of deprecated temporary addresses can have an impact on storage usage.

VALIDLIFETIME default_*valid_lifetime*
Specifies the default valid lifetime for temporary addresses in hours. The default is 7 times the preferred lifetime; you can specify a maximum value of 90 days.

Steps for modifying

To modify most parameters for the IPCONFIG6 statement, you must respecify the statement with the new parameters. Additional actions are required to modify the following parameters:

CHECKSUMOFFLOAD | NOCHECKSUMOFFLOAD
If the CHECKSUMOFFLOAD or NOCHECKSUMOFFLOAD parameter is changed with the VARY TCPIP,,OBEYFILE command, the new value does not affect any active OSA-Express QDIO interfaces. For this change to affect an active OSA-Express QDIO interface, the interface must be stopped and restarted.

DYNAMICXCF
None of the parameters on the IPCONFIG6 DYNAMICXCF statement can be changed with a VARY TCPIP,,OBEYFILE command. You must first stop the TCP/IP stack, apply changes, and then restart the TCP/IP stack.

If dynamic XCF definitions have been enabled but a later VARY TCPIP,,OBEYFILE command contains NODYNAMICXCF, only future dynamic definitions and connectivity are affected. Existing definitions and connectivity are not affected.

IPSECURITY
z/OS IPv6 IPSec functions cannot be activated using the VARY TCPIP,,OBEYFILE command on an active TCP/IP stack. To activate z/OS IPSec for IPv6, halt all traffic on the designated TCP/IP stack, stop the stack, modify the TCP profile to include IPCONFIG6 IPSECURITY, and restart the stack.

MULTIPATH
If you modify the multipath routing type (PERCONNECTION to PERPACKET, or vice versa), the new parameter takes effect only for new connections created after the modification is done, and existing connections use whatever the value was when the connection was established. If you enable multipath routing when it was previously disabled, existing connections are not affected; multipath routing is applied to new connections only.

SEGMENTATIONOFFLOAD | NOSEGMENTATIONOFFLOAD
If the SEGMENTATIONOFFLOAD or NOSEGMENTATIONOFFLOAD parameter is changed with the VARY TCPIP,,OBEYFILE command, the new value does not affect any active OSA-Express QDIO interfaces. For this change to affect an active OSA-Express QDIO interface, the interface must be stopped and restarted.

TEMPADDRS
If you disable temporary addresses by changing TEMPADDRS to NOTEMPADDRS using a VARY TCPIP,,OBEYFILE command, all existing IPv6 temporary addresses are deleted. This is disruptive for connections that are using the temporary address.

Related topics

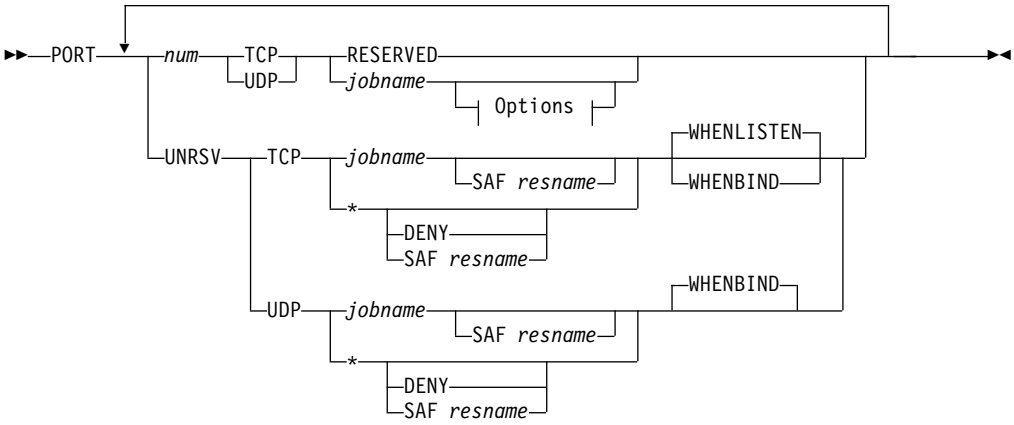
- "GLOBALCONFIG statement" on page 55
- "IPCONFIG statement" on page 116
- SRCIP statement

PORT statement

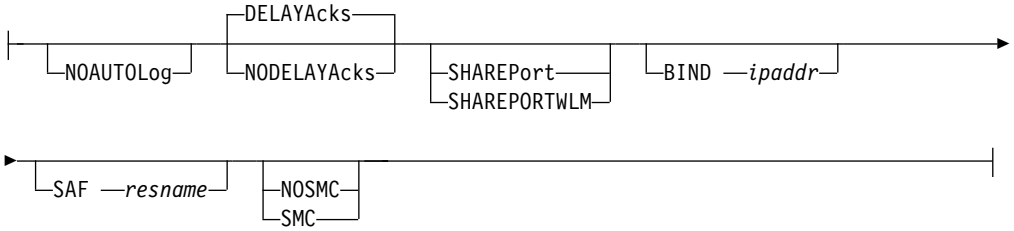
Use the PORT statement to reserve a port for one or more specified job names or to control application access to unreserved ports.

Syntax

Rule: The PORT parameters and options (for example, NOAUTOLOG, DELAYACKS) must be specified in the order in which they appear on the following syntax diagram.



Options:



Parameters

num

The number of the port to be reserved. The same port number can appear in more than one PORT statement with different users or more than once in the same PORT statement. This port cannot appear in a range specified by the PORTRANGE statement. If a PORTRANGE statement including this port number is specified prior to this statement, this port is ignored. If the PORTRANGE statement follows this statement, the PORTRANGE statement is ignored. An error message is generated in either case. *num* is a value in the range 1 - 65535.

Requirement: For z/OS UNIX applications that are invoked by INETD, ensure that the port number defined for the application in the /etc/services file is the same as the port number reserved for the application on the PORT statement.

UNRSV

This value indicates any unreserved port (any port number that is in the range 1 - 65535 that has not been reserved by a PORT or PORTRANGE statement).

Use PORT UNRSV statements to indicate which applications or users are permitted to access application-specified unreserved ports. PORT UNRSV statements control access to all unreserved ports in the range 1 - 65535 unless RESTRICTLOWPORTS is configured; however, when RESTRICTLOWPORTS is configured, PORT UNRSV statements control access to unreserved ports only above port 1023. For UDP, access control is applied when an application issues a bind to a particular port number to establish a local port. For TCP, access control is applied depending on the value of the WHENBIND or WHENLISTEN parameter.

If neither DENY nor the SAF keyword is specified, an application that matches the protocol and specified job name [the job name can be an asterisk (*)] on a PORT UNRSV statement can access unreserved ports. If DENY is specified, all applications are denied access to unreserved ports for the specified protocol. If the SAF keyword is specified, applications that match the PORT UNRSV statement must also have user access to the SAF SERVAUTH resource which is indicated by the SAF keyword, to be permitted to access an unreserved port.

Results:

- When no PORT UNRSV statements are configured for the socket protocol that is being used, all applications are allowed access to the unreserved ports unless prevented by TCPCONFIG or UDPCONFIG RESTRICTLOWPORTS or by GLOBALCONFIG EXPLICITBINDPORTRANGE. This is the default.
- When TCPCONFIG or UDPCONFIG RESTRICTLOWPORTS is configured for the access protocol that is being used, PORT UNRSV access control applies only to unreserved ports above port 1023.
- If any PORT UNRSV statements are configured for a protocol, access is determined by the PORT UNRSV statement whose specified job name most closely matches the application's job name. If the application's *jobname* does not match any of the PORT UNRSV statements, the application's access to unreserved ports is denied for that protocol.
- PORT UNRSV statements control access to nonzero, unreserved ports that are specified on explicit binds. Access to unreserved ports that are assigned by the stack is not affected.

Guideline: In a Common INET (CINET) environment with multiple stacks and no established stack affinity, an explicit bind to port 0 is converted to a bind to a specific port in the CINET range. If you have not reserved the ports in your CINET range for *jobname* OMVS, the explicit bind to port 0 is treated as an explicit bind to an unreserved port.

RESERVED
Indicates the port is not available for use by any user. Use RESERVED to lock certain ports. This is optional and valid for TCP or UDP protocols.

jobname
Specifies the MVS job name that can use the specified port or any unreserved port in the case of a PORT UNRSV statement. You can specify the *jobname* value as one of the following values:

- The 1- through 8-character name of the job that is required to use the port.
- An asterisk (*) wildcard value. Specify an asterisk as the *jobname* value to reserve a port without specifying a particular job name. You can use an asterisk if you do not know the exact job name or if you want to allow different applications to serially bind to the port.
- A 1- through 7-character prefix that is followed by an asterisk wildcard value. This specification enables all job names that match the prefix to access the port.

For UDP, only one job name can be associated with a particular port. For TCP, the same port can be reserved multiple times for different job names. This can be useful if you have different servers with different job names that need access to the same port. For PORT UNRSV statements, both TCP and UDP can have multiple statements with different job names.

For multiple TCP reservations for the same port, or for multiple PORT UNRSV statements for the same protocol, the TCP/IP stack searches these PORT statements for the closest match (if any) to the application's job name. If you

specified the job name using a wildcard on more than one of these statements, the TCP/IP stack matches the application job name to a PORT statement *jobname* value using the most specific value first and the least specific value (or value *, if it was specified) last.

Restriction: To reserve a port that is to be monitored by AUTOLOG, the *jobname* name must exactly match (no wildcards) the *jobname* name on the AUTOLOG statement.

The environment in which the application is run determines the job name to be associated with a particular client or server application.

The following list explains how to determine the *jobname* value given the environment in which the application is run:

- Applications run from batch use the batch job name.
- Applications started from the MVS operator console use the started procedure name as the job name.
- Applications run from a TSO user ID use the TSO user ID as the job name.
- Applications run from the z/OS shell normally have a job name that is the logged on user ID plus a one-character suffix.
- Authorized users can run applications from the z/OS shell and use the _BPX_JOBNAME environment variable to set the job name. In this case, the value specified for the environment variable is the job name.
- Use the name of the started JCL procedure for the UNIX System Services kernel address space to enable applications (except for applications using the Pascal API) to bind to the port. This name is typically OMVS unless a different name is explicitly specified in the STARTUP_PROC parameter of the BPXPRMxx parmlib member.
- z/OS UNIX applications started by INETD use the *jobname* of the INETD server.
- Use the name of the VTAM started task for the UDP ports that are to be used for Enterprise Extender (EE) network connections.

  Restriction: The VTAM job name cannot include a wildcard character (*) when it reserves EE UDP ports.

Reserved Port Options:

NOAUTOLOG

Tells the TCP/IP address space *not* to restart the server if it was stopped previously. Otherwise, the default is to restart the server if it was stopped previously. If the application associated with the job name is an AUTOLOG started procedure, and the port is inactive (for TCP connections, the procedure must have a socket open to that port in the LISTEN state; for UDP connections, the procedure must have a socket open to that port), then AUTOLOG assumes that the procedure is hung; it cancels and restarts it every five minutes. Use NOAUTOLOG to prevent this from occurring. See AUTOLOG statement for more information.

DELAYACKS | NODELAYACKS

DELAYACKS

Delays transmission of acknowledgments when a packet is received with the PUSH bit on in the TCP header. The DELAYACKS parameter on the PORT statement affects only connections that use this port. This is the default, but the behavior can be overridden by specifying the

NODELAYACKS parameter on the TCP/IP stack TCPCONFIG profile statement, or on any of the following statements used to configure the route used by the TCP connection:

- The TCP/IP stack BEGINROUTES profile statement
- The Policy Agent RouteTable statement
- The OMPROUTE configuration statements

NODELAYACKS
Specifies that an acknowledgment is returned immediately when a packet is received with the PUSH bit on in the TCP header. The NODELAYACKS parameter on the PORT statement affects only connections that use this port. Specifying NODELAYACKS on the PORT statement overrides the specification of the DELAYACKS parameter on the TCP/IP stack TCPCONFIG profile statement or on any of the following statements used to configure the route used by the TCP connection:

- The TCP/IP stack BEGINROUTES profile statement
- The Policy Agent RouteTable statement
- The OMPROUTE configuration statements

SHAREPORT
Required when reserving a port to be shared across multiple listeners on the same interface. When SHAREPORT is specified, TCP/IP allows multiple listeners to listen on the same combination of port and IP address.

As incoming client connections arrive for this port and IP address, TCP/IP distributes them across the listeners. Specification of this keyword causes incoming connection requests for the port to be distributed among the listeners using a weighted round-robin distribution method based on the servers' accept Efficiency Fractions (SEFs) of the listeners sharing the port. The SEF is a measure, calculated at intervals of approximately one minute, of the efficiency of the server application in accepting new connection requests and managing its backlog queue. Alternatively, SHAREPORTWLM can be coded instead; SHAREPORTWLM changes the connection distribution algorithm.

If the same port is reserved for multiple job names, SHAREPORT or SHAREPORTWLM needs to be specified on only one instance of the port reservation. SHAREPORTand SHAREPORTWLM are valid only for TCP ports. The last setting of either SHAREPORT or SHAREPORTWLM is used for all TCP/IP servers that use that port.

SHAREPORTWLM
Required when reserving a port to be shared across multiple listeners on the same interface. When SHAREPORTWLM is specified, TCP/IP allows multiple listeners to listen on the same combination of port and IP address.

The SHAREPORTWLM option can be used instead of SHAREPORT. Like SHAREPORT, SHAREPORTWLM causes incoming connections to be distributed among a set of TCP listeners; however, unlike SHAREPORT, the listener selection is based on WLM server-specific recommendations, modified by the SEF values for each listener. WLM server-specific recommendations are acquired at intervals of approximately 1 minute from the Work Load Manager and reflect the listener's capacity to handle additional work.

If the same port is reserved for multiple job names, SHAREPORT or SHAREPORTWLM needs to be specified on only one instance of the port

reservation. SHAREPORT and SHAREPORTWLM are valid only for TCP ports. The last setting of either SHAREPORT or SHAREPORTWLM is used for all TCP/IP servers that use that port.

Result: zAAP and zIIP processor capacity is automatically included when the SHAREPORTWLM parameter is specified and all systems in the sysplex are V1R9 or later.

BIND *ipaddr*
Associates a job name with the IP address, *ipaddr*. When a job with the designated name binds to the IPv4 INADDR_ANY address, or to the IPv6 unspecified address (in6addr_any), the bind is intercepted and converted to a bind to the IP address specified by *ipaddr*. Subsequent bind processing occurs as though the server instance had originally issued the bind to the IP address *ipaddr*.

You can specify either an IPv4 address (in dotted decimal notation) or an IPv6 address (in hexadecimal notation). IPv4-mapped IPv6 addresses and IPv6 addresses with the reserved prefix ::/96 are not supported.

Rule: The BIND *ipaddr* parameter does not apply to the PORTRANGE statement.

Guidelines:

- When you are using the BIND parameter with IPv6 addresses, you should use only manually configured addresses, because autoconfigured addresses might change when the stack is recycled.
- If the IP address specified on the BIND parameter is also specified in a VIPARANGE statement subnet, then VIPARANGE security verification might occur to determine whether an application can create the dynamic VIPA (DVIPA). For information about security profiles for binding to DVIPAs in the VIPARANGE statement, see z/OS Communications Server: IP Configuration Guide.

SAF *resname*
Indicates that the port is reserved for users that have READ access to the RACF resource

```
EZB.PORTACCESS.sysname.tcpname.resname
```

where

- EZB.PORTACCESS is constant
- *sysname* is the value of the MVS &SYSNAME. system symbol
- *tcpname* is the name of the procedure used to start the TCP stack
- *resname* is the 1-8 character value following the SAF keyword

Restriction: You can not specify a 1-character value of 0 (zero) for *resname*.

If the SAF keyword is specified and a user tries to bind to the port and is not allowed access to the resource, the BIND socket call fails.

Tip: The SAF keyword is ignored when VTAM opens a UDP port for Enterprise Extender (EE) network connections. However, it can still be used to prevent other address spaces that are using the same name as the VTAM started task from opening the port.

This is optional and valid for TCP or UDP protocols.

If the *jobname* parameter is specified as an asterisk (*), any user ID that is RACF-permitted to the resource specified by the *resname* value is allowed to bind to the port specified by the value; APF or superuser authority is not required.

This permits multiple users access to the protected port. However, the stack allows only one user to actually BIND to the port at a time. Use SHAREPORT or SHAREPORTWLM to override this behavior for TCP ports.

Guideline: If an application binds to an IP address that is also specified in a VIPARANGE statement subnet, then additional security verification might occur to determine whether the application can create the dynamic VIPA (DVIPA). This additional verification might occur whether the application explicitly binds to the DVIPA address or whether the application binds to the unspecified address and is converted to the DVIPA address using the BIND parameter. For information about security profiles for binding to DVIPAs in the VIPARANGE statement, see z/OS Communications Server: IP Configuration Guide.

SMC | NOSMC
Configuration of these parameters overrides configuration of the AUTOSMC monitoring function for the servers that are associated with the reserved port. The AUTOSMC monitoring function is the default option for the GLOBALCONFIG SMCGLOBAL parameter. However, the default AUTOSMC monitoring is activated only when you enable SMC. For more information about enabling SMC, see the description of the GLOBALCONFIG SMCR and SMCD parameters. For more information about AUTOSMC monitoring function, see Use the AUTOSMC monitoring function in z/OS Communications Server: IP Configuration Guide.

NOSMC
Indicates that Shared Memory Communications (SMC) is not permitted for inbound TCP connections that use this port. This setting overrides the SMCGLOBAL AUTOSMC parameter on the GLOBALCONFIG profile statement and ensures that inbound TCP connections to this port do not use SMC. NOSMC is valid only for TCP ports.

SMC Indicates that the stack attempts to use SMC for inbound TCP connections that use this port. This parameter is required only when you use the SMCGLOBAL AUTOSMC parameter on the GLOBALCONFIG profile statement and you want to ensure that the stack attempts to use SMC for inbound TCP connections. SMC is valid only for TCP ports.

Unreserved Port Options:

SAF *resname*
Indicates that binding to, or listening on, any unreserved port is restricted to users that are permitted to the specified SAF SERVAUTH resource. See the description of the SAF parameter for more information.

DENY
DENY indicates that port access should be denied. DENY can be specified only for unreserved ports (on the PORT UNRSV statement) and only when the specified jobname is an asterisk (*).

A PORT UNRSV *protocol* * DENY statement is needed only if no other PORT UNRSV statements are configured for the specified protocol and you want to prevent all access to unreserved ports using that protocol.

WHENLISTEN
WHENLISTEN indicates that port access control is targeted to TCP applications that are acting as servers (that is, applications able to accept incoming client TCP connections) that issue an explicit bind to a user-specified unreserved port. Permission to use the unreserved port is determined when a TCP listen is issued. If a listen is not issued, no access control check is made. The WHENLISTEN parameter is not available for the UDP protocol, and it is the default for the TCP protocol.

Rule: Every PORT UNRSV statement for the TCP protocol must use the same access control option. You cannot specify, or default to, the WHENLISTEN parameter on some statements and specify the WHENBIND parameter on other statements.

WHENBIND
WHENBIND indicates that permission to use an unreserved port is determined when an explicit bind to a specific local port is issued. This is the default, and only option, for the UDP protocol, and it can affect UDP applications that bind to a specific local port. If the WHENBIND parameter is specified for the TCP protocol, it can affect TCP client applications that bind to a specific local port for outbound connections.

Rule: Every PORT UNRSV statement for the TCP protocol must specify, or default to, the same access control option. You cannot specify the WHENLISTEN parameter on some statements and specify the WHENBIND parameter on other statements.

Steps for modifying

To change a parameter value, you must delete the existing PORT statement by using the DELETE PORT statement, then redefine with the new PORT statement.

Examples

The following example was used for test configuration and is provided here for illustration only. The sample profile, SEZAINST(SAMPPROF), contains the most current assignments.

```
PORT
     7 UDP MISCSERV           ; Miscellaneous Server - echo
     7 TCP MISCSERV           ; Miscellaneous Server - echo
     9 UDP MISCSERV           ; Miscellaneous Server - discard
     9 TCP MISCSERV           ; Miscellaneous Server - discard
    19 UDP MISCSERV           ; Miscellaneous Server - chargen
    19 TCP MISCSERV           ; Miscellaneous Server - chargen
    20 TCP *  NOAUTOLOG       ; FTP Server
;   20 TCP *  NOAUTOLOG SAF FTPDATA ; FTP Server
    21 TCP FTPD1              ; FTP Server
    23 TCP TN3270             ; Telnet 3270 Server
;   23 TCP INETD1 BIND 9.67.113.3 ; z/OS UNIX Telnet server
    25 TCP SMTP               ; SMTP Server
   111 TCP PORTMAP            ; Portmap Server (SUN 3.9)
   111 UDP PORTMAP            ; Portmap Server (SUN 3.9)
;  111 TCP PORTMAP1           ; Unix Portmap Server (SUN 4.0)
;  111 UDP PORTMAP1           ; Unix Portmap Server (SUN 4.0)
   123 UDP SNTPD              ; Simple Network Time Protocol Server
   135 UDP LLBD               ; NCS Location Broker
   161 UDP OSNMPD             ; SNMP Agent
   389 TCP LDAPSRV            ; LDAP Server
   443 TCP HTTPS              ; http protocol over TLS/SSL
   443 UDP HTTPS              ; http protocol over TLS/SSL
;  500 UDP IKED               ; CS IKE daemon
```

```
   512 TCP RXSERVE             ; Remote Execution Server
   514 TCP RXSERVE             ; Remote Execution Server
;  512 TCP * SAF OREXECD       ; z/OS UNIX Remote Execution Server
;  514 TCP * SAF ORSHELLD      ; z/OS UNIX Remote Shell Server
;  515 TCP LPSERVE             ; LPD Server
;  515 TCP AOPLPD              ; Infoprint LPD Server
   520 UDP OMPROUTE            ; OMPROUTE Server (IPv4 RIP)
   521 UDP OMPROUTE            ; OMPROUTE Server (IPv6 RIP)
   750 TCP MVSKERB             ; Kerberos
   750 UDP MVSKERB             ; Kerberos
   751 TCP ADM@SRV             ; Kerberos Admin Server
   751 UDP ADM@SRV             ; Kerberos Admin Server
; 1700 TCP PAGENT NOAUTOLOG    ; Policy Agent pagentQosListener port
; 1701 TCP PAGENT NOAUTOLOG    ; Policy Agent pagentQosCollector port
  3000 TCP CICSTCP             ; CICS Socket
  3389 TCP MSYSLDAP            ; LDAP Server for Msys
; 4159 TCP NSSD                ; CS NSS daemon
; 4500 UDP IKED                ; CS IKE daemon
;16310 TCP PAGENT NOAUTOLOG    ; Policy Agent server listener port
;
```

The following examples control application access to unreserved ports:

- To deny all TCP explicit binds to an unreserved port, add the following statement to your profile:

  ```
  PORT  UNRSV  TCP  *  DENY WHENBIND
  ```

- To allow TCP explicit binds to an unreserved port but deny all TCP listens on an unreserved port, add the following statement to your profile:

  ```
  PORT  UNRSV  TCP  *  DENY  WHENLISTEN
  ```

- To deny all TCP listens on an unreserved port, except for applications that match *jobname* value ABC*, add the following statement to your profile:

  ```
  PORT  UNRSV  TCP  ABC*   WHENLISTEN
  ```

  Guideline: If the ports that applications ABC* are accessing are predictable, you should use PORT reservation statements for those specific ports instead of using the PORT UNRSV statement.

- To deny all TCP listens on an unreserved port, except for application MYAPP1 and all users permitted to EZB.PORTACCESS.*sysname.tcpname*.GENERIC, add the following statements to your profile:

  ```
  PORT  UNRSV  TCP  MYAPP1
  PORT  UNRSV  TCP  *  SAF  GENERIC
  ```

- To deny all UDP explicit binds to an unreserved port, except for users permitted to EZB.PORTACCESS.*sysname.tcpname*.GENERIC, add the following statement to your profile:

  ```
  PORT  UNRSV  UDP  *  SAF  GENERIC
  ```

Usage notes

- If there are no PORT UNRSV statements configured for this stack, any user can use a port that is not reserved in this list or that is not reserved with the PORTRANGE statement. If you have TCP/IP hosts in your network that use ports in the range 1 - 1023 for privileged applications, you should reserve them with this statement, the PORTRANGE statement, or the RESTRICTLOWPORTS parameter on the TCPCONFIG or UDPCONFIG statements.
- If an application attempts to access a specific port by explicitly binding for UDP, by explicitly binding, or listening for TCP, and no PORT or PORTRANGE statement is found that matches that port and protocol (that is, the port is unreserved for that protocol), then a check is made for PORT UNRSV statements. The following list shows the possible results:

  - If there are no PORT UNRSV statements for that protocol, the access is allowed.
  - If there are any PORT UNRSV statements for the protocol, a search is made for the most specific match to the application's job name.
    - If a match is found, the access is allowed unless the closest matching PORT UNRSV statement contains the DENY keyword, or if it contains the SAF keyword and the user is not permitted to the specified SAF resource.
    - If no matching PORT UNRSV statement is found, the access is denied.
- For z/OS UNIX applications, you can reserve a port by specifying the job name of the application or you can use the name of the started JCL procedure for the z/OS UNIX kernel address space to enable any application (except applications using the Pascal API) to bind to the port. This name is typically OMVS unless a different name is explicitly specified in the STARTUP_PROC parameter in the BPXPRMxx parmlib member. See z/OS MVS Initialization and Tuning Reference for more details about the STARTUP_PROC parameter.
- For syslogd, you must include the following PORT statement:

```
PORT
    514 UDP OMVS         ; syslogd Server
```

  This port is required for syslogd to accept log data from remote syslogd servers.

  Guideline: Instead of OMVS, you can also use the job name of the syslog daemon on this port reservation statement. If your syslog daemon's job name is SYSLOGD1, you can specify:

```
PORT   514   UDP   SYSLOGD1
```

- If you want SNMP OSA Management support, see z/OS Communications Server: IP Configuration Guide for more information about the PORT statement.
- The NOSMC option is enforced during TCP bind() processing. To allow servers that bind to a port that is configured with the NOSMC option to use SMC communications, you need to perform the following steps:
  1. Delete the existing port reservation by using the VARY TCPIP,,OBEYFILE command with a data set that contains a DELETE PORT statement.
  2. Create a reservation for the port by using the VARY TCPIP,,OBEYFILE command with a data set that contains a PORT statement without the NOSMC parameter.
  3. Stop and restart the servers that use the port.

Related topics

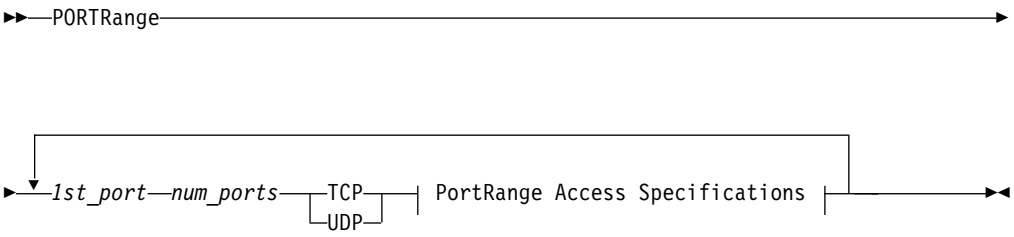
- AUTOLOG statement
- DELETE statement
- "GLOBALCONFIG statement" on page 55
- "PORTRANGE statement"
- TELNETPARMS statements

PORTRANGE statement

Use the PORTRANGE statement to reserve a range of ports for specified user IDs, procedures, or job names. The PORTRANGE statement can also specify other options that apply to all ports in the range.

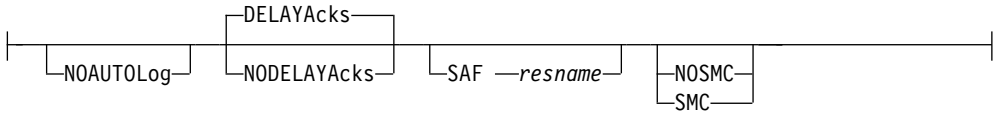
Rule: The portrange options (NOAUTOLOG, DELAYACKS, and so on) must be specified in the same order as they appear on the following syntax diagram.

Syntax



PortRange Access Specifications:

Options:



Parameters

1st_port
The starting port for a range of ports to reserve. The same port number cannot appear in multiple PORTRANGE statements, nor can the port be specified on both PORTRANGE and PORT statements. If the port is specified on a PORT statement prior to this statement, this port range is ignored. If the port is specified on a PORT statement that follows this statement, the port in the PORT statement is ignored. An error message is generated in either case. *1st_port* is a value in the range 1 - 65535.

If the *1st_port* and *num_ports* values that are specified result in a range of ports that exceeds the maximum port number of 65535, the ports up to 65535 are reserved and those greater than 65535 are ignored.

num_ports
The number of ports to reserve. The ports reserved cannot overlap other ranges specified by a PORTRANGE statement. No ports within this range can be specified on a PORT statement. If the port is specified on a PORT statement prior to this statement, this port range is ignored. If the port is specified on a PORT statement that follows this statement, the port in the PORT statement is ignored. An error message is generated in either case. *num_port* is a value in the range 1 - 65535.

If the *1st_port* and *num_ports* values that are specified result in a range of ports that exceeds the maximum port number of 65535, the ports up to 65535 are reserved and those greater than 65535 are ignored.

jobname
The MVS job name that can use the port. You can specify the *jobname* value as 1 - 8 characters, an asterisk (*) wildcard value, or a 1 - 7 character prefix followed by an asterisk wildcard value. Specify an asterisk as the *jobname* value

to reserve a port without specifying a particular job name. This is useful when you do not know the exact job name or when you want to allow several different applications to serially bind to the port. Specify a 1 - 7 character prefix followed by an asterisk to enable all job names that match the prefix to access the ports in the range.

Restrictions:

- For UDP, only one job name can be associated with a port.
- To reserve a port that is to be monitored by the AUTOLOG function, the *jobname* value must exactly match the *jobname* value on the AUTOLOG statement; you cannot use an asterisk wildcard value.

Guideline: If a TCP port is to be shared by multiple users, use the PORT statement instead. The PORTRANGE statement does not support sharing of ports.

Determining the job name to be associated with a particular client or server application depends on the environment in which the application is run.

- Applications run from batch use the batch job name.
- Applications started from the MVS operator console use the started procedure name as the job name.
- Applications run from a TSO user ID use the TSO user ID as the job name.
- Applications run from the z/OS shell normally have a job name that is the logged on user ID plus a 1-character suffix.
- Authorized users can run applications from the z/OS shell and use the _BPX_JOBNAME environment variable to set the job name. In this case, the value specified for the environment variable is the job name.
- Use the name of the started JCL procedure for the UNIX System Services kernel address space to enable any application (except for applications using the Pascal API) to bind to the port. This name is typically OMVS unless a different name is explicitly specified in the STARTUP_PROC parameter in the BPXPRMxx parmlib member.
- To reserve the port and not allow any application access to it, use the name RESERVED.
- To reserve ports for the FTP server's use as passive data ports, use the name AUTHPORT and the protocol TCP. You must also code the PASSIVEDATAPORTS value in the FTP server's FTP.DATA data set.
- Use the name of the VTAM started task for the UDP ports that are to be used for Enterprise Extender (EE) network connections.

  Restriction: The VTAM jobname can NOT include a wildcard character (*) when it reserves EE UDP ports.

RESERVED
Indicates that all ports in the port range are not available for use by any user.

AUTHPORT
Indicates that all ports in the port range are not available for use by any user except FTP, and only when FTP is configured to use PASSIVEDATAPORTS. AUTHPORT is valid only with the TCP protocol.

NOAUTOLOG
Tells the TCP/IP address space *not* to restart the server if it was stopped previously. Otherwise, the default is to restart the server if it was stopped previously.

DELAYACKS | NODELAYACKS

NODELAYACKS
Specifies that an acknowledgment is returned immediately when a packet is received with the PUSH bit on in the TCP header. The NODELAYACKS parameter on the PORTRANGE statement, affects only connections that use this port. Specifying the NODELAYACKS parameter on the PORTRANGE statement overrides the specification of the DELAYACKS parameter on the TCP/IP stack TCPCONFIG profile statement, or on any of the following statements used to configure the route used by the TCP connection:

- The TCP/IP stack BEGINROUTES profile statement
- The Policy Agent RouteTable statement
- The OMPROUTE configuration statements

DELAYACKS
Delays transmission of acknowledgments when a packet is received with the PUSH bit on in the TCP header. The DELAYACKS parameter on the PORTRANGE statement affects only connections that use this port. This is the default, but the behavior can be overridden by specifying the NODELAYACKS parameter on the TCP/IP stack TCPCONFIG profile statement, or on any of the following statements used to configure the route used by the TCP connection:

- The TCP/IP stack BEGINROUTES profile statement
- The Policy Agent RouteTable statement
- The OMPROUTE configuration statements

SAF *resname*
SAF *resname* indicates that all ports in the range are reserved for users that have READ access to the RACF resource.

```
EZB.PORTACCESS.sysname.tcpname.resname
```

where

- EZB.PORTACCESS is constant
- *sysname* is the value of the MVS &SYSNAME. system symbol
- *tcpname* is the name of the procedure used to start the TCP stack
- *resname* is a 1-8 character value following the SAF keyword

Restriction: You can not specify a 1-character value of 0 (zero) for *resname*.

If the SAF keyword is specified and an application tries to bind to a port in the port range, and the user ID associated with the application is not permitted to the resource, the BIND socket call fails.

This is optional and valid for TCP or UDP protocols.

If the *jobname* value is specified as an asterisk (*), any user ID that is RACF-permitted to the resource specified by the *resname* value is allowed to bind to the port; APF or superuser authority is not required.

Guideline: If an application binds to an IP address that is also specified in a VIPARANGE statement subnet, then additional security verification might occur to determine whether the application can create the dynamic VIPA (DVIPA). For information about security profiles for binding to DVIPAs in the VIPARANGE statement, see z/OS Communications Server: IP Configuration Guide

SMC | NOSMC
Configuration of these parameters overrides configuration of the AUTOSMC

monitoring function for the servers that are associated with the reserved port. The AUTOSMC monitoring function is the default option for the GLOBALCONFIG SMCGLOBAL parameter. However, the default AUTOSMC monitoring is activated only when you enable SMC. For more information about enabling SMC, see the description of the GLOBALCONFIG SMCR and SMCD parameters. For more information about AUTOSMC monitoring function, see Use the AUTOSMC monitoring function in z/OS Communications Server: IP Configuration Guide.

NOSMC
Indicates that Shared Memory Communications (SMC) is not permitted for TCP connections that use any port in this range. This setting overrides the SMCGLOBAL AUTOSMC parameter on the GLOBALCONFIG profile statement and ensures that inbound TCP connections to any port in this range do not use SMC. NOSMC is valid only for TCP ports.

SMC Indicates that the stack attempts to use SMC for inbound TCP connections that use any port in this range. This parameter is required only when you use the SMCGLOBAL AUTOSMC parameter on the GLOBALCONFIG profile statement and you want to ensure that the stack attempts to use SMC for inbound TCP connections. SMC is valid only for TCP ports.

Steps for modifying

To change a parameter value, you must delete the existing PORTRANGE statement by using the DELETE PORTRANGE statement, then redefine the parameter with the new PORTRANGE statement.

Examples

This example shows a PORTRANGE statement used to reserve a large number of ports for a single test system.

```
PORTRANGE
    4000 200  TCP TESTSYS
```

The following example shows a PORTRANGE statement that reserves port 111 for both UDP and TCP for one user, ports 500 - 504 for two different users, one using UDP and one using TCP, and ports 700 - 703 for TCP users with job names that begin with the prefix ABCD.

```
PORTRANGE
     111   1  UDP  PORTMAP
     111   1  TCP  PORTMAP
     500   5  UDP  USER1
     500   5  TCP  USER2
     700   4  TCP  ABCD*
```

Usage notes

- A range of ports specified in a VARY TCPIP,,OBEYFILE command data set are added to the list of ports already reserved.
- Any user can use a port that is not reserved by a PORT or PORTRANGE statement. If you have TCP/IP hosts in your network that reserve ports in the range 1 - 1023 for privileged applications, you should reserve them either with this statement, the PORT statement, or the RESTRICTLOWPORTS parameter on the TCPCONFIG or UDPCONFIG statements.

- If you are reserving ports for the INADDRANYPORT() parameter in the BPXPRMxx SYS1.PARMLIB member, you must specify the name of the started JCL procedure for the z/OS UNIX kernel address space to enable any application (except for applications using the Pascal API) to bind to the port. This name is typically OMVS unless a different name is explicitly specified in the STARTUP_PROC parameter in the BPXPRMxx parmlib member. See z/OS MVS Initialization and Tuning Reference for more details about the STARTUP_PROC parameter. You can use IBM Health Checker for z/OS enhancements to check whether the range of ports specified by the INADDRANYPORT and INADDRANYCOUNT parameter of the BPXPRMxx parmlib member is reserved for OMVS on the TCP/IP stack when operating in a CINET environment. For more details about IBM Health Checker for z/OS enhancements, see the IBM Health Checker for z/OS enhancements information in the z/OS Communications Server: IP Diagnosis Guide
- The NOSMC option is enforced during TCP bind() processing. To allow servers that bind to a port in this range that is configured with the NOSMC option to use SMC communications, you need to perform the following steps:
  1. Delete the existing port reservations by using the VARY TCPIP,,OBEYFILE command with a data set that contains a DELETE PORTRANGE statement.
  2. Create reservations for the port by using the VARY TCPIP,,OBEYFILE command with a data set that contains a PORTRANGE statement without the NOSMC parameter.
  3. Stop and restart the servers that use the ports.

Related topics

- DELETE statement
- PASSIVEDATAPORTS (FTP server) statement
- "GLOBALCONFIG statement" on page 55
- "PORT statement" on page 144

Chapter 4. IP Programmer's Guide and Reference

SMF type 119 records

SMF type 119 records contain unique stack identification sections designed to eliminate the confusion of the type 118 records. They provide uniformity of date and time (UTC), common record format (self-defining section and TCP/IP identification section), and support for IPv6 addresses and expanded field sizes (64 bit versus 32 bit) for some counters. The following kinds of SMF type 119 records are available:

- TCP connection initiation and termination
- UDP socket close
- TCP/IP interface and server port statistics
- TCP/IP stack start/stop
- FTP server transfer completion
- FTP server logon failure
- FTP client transfer completion
- TN3270E Telnet server session initiation and termination
- Telnet client connection initiation and termination
- IKE tunnel activation, refresh, and expire
- Dynamic tunnel activation, refresh, installation, and removal
- Manual tunnel activation and deactivation
- TCP/IP profile
- TN3270E Telnet server profile
- CSSMTP processing of configuration files, spool files, mail messages, connections and statistical records
- DVIPAs and sysplex distributor targets
- Shared Memory Communication - RDMA (SMC-R) link initiation and termination
- SMC-R link, link group, and interface statistics

The SMF type 119 records utilize a common structure. Each record is organized as follows:

- SMF header
- Self-defining section containing pointers to:
  - TCP/IP identification section (identifies system, stack etc)
  - Sections containing the data for the record

You can parse the SMF type 119 records that TCP/IP generates by using macros and header files.

- For assembler applications, use the following macros:
  - EZASMF77, which is installed in SYS1.MACLIB.
  - EZBNMMPA, which is installed in TCP/IP data set SEZANMAC. This macro is needed only for the TCP/IP profile record.
- For C/C++ applications, use the following header files:
  - ezasmf.h

– ezbnmmpc.h

This header file is needed only for the TCP/IP profile record.

These header files are installed in TCP/IP data set SEZANMAC, and in the /usr/include file system directory.

The OpenSSH element of z/OS also creates SMF 119 records. The EZASMF77 macro and the ezasmf.h header file contain reserved SMF 119 record subtype definitions for these records. For a description of these records, see z/OS OpenSSH User's Guide.

TCP/IP callable NMI (EZBNMIFR)

z/OS Communications Server provides a high-speed low-overhead callable programming interface for network management applications to access data related to the TCP/IP stack. Use the EZBNMIFR network management interface to perform the following functions:

- Drop one or more TCP connections
- Drop one or more UDP endpoints
- Monitor Shared Memory Communications over Remote Direct Memory Access link groups and links within each group
- Monitor Shared Memory Communications - Direct Memory Access (SMC-D) links
- Monitor TCP or UDP endpoints
- Monitor TCP/IP stack interface and global statistics
- Monitor TCP/IP stack profile statement settings
- Monitor TCP/IP storage
- Monitor TCP/IP sysplex networking data
- Monitor TN3270E Telnet server performance
- Obtain configuration data of active FTP daemons
- Obtain configuration data of active TN3270E severs

This section describes the details for invoking the EZBNMIFR interface with the defined input parameters and for processing the output it provides. The following topics are addressed:

- EZBNMIFR overview
- EZBNMIFR: Configuration and enablement
- Using the EZBNMIFR requests
- TCP/IP NMI request format
- "TCP/IP NMI response format" on page 172
- TCP/IP NMI request and response data structures
- TCP/IP NMI examples

EZBNMIFR: Poll-type requests

For poll-type requests, EZBNMIFR is a callable interface that returns data related to the TCP/IP stack at a given point in time. In most cases, the caller can specify filters that limit the returned data to a specific set of information.

Poll-type requests enable you to obtain the following types of information from the TCP/IP stack:

- Active TCP connections

- Active UDP endpoints
- Active TCP listeners
- TCP/IP storage utilization
- TN3270E Telnet server monitor groups
- TN3270E Telnet server connection performance data
- Sysplex XCF data
- Dynamic VIPA addresses
- Dynamic VIPA port distribution
- Dynamic VIPA routes
- Dynamic VIPA connections
- TCP/IP profile statement settings
- Interface attributes and IP addresses
- Interface standard and extended statistics
- TCP/IP stack global statistics
- FTP daemon configuration
- TN3270E Telnet server profile statement settings
- Active SMC-R link groups and links within each group
- Active SMC-D links

Format and details for poll-type requests

The following poll-type requests are provided by EZBNMIFR. The request constant, which is specified in the NWMType field in the NWMHeader data structure, follows the request name. Some requests support filters. See "Filter request section" on page 166 for a description of each filter and the information about which filters are supported by each request. For more information about Shared Memory Communications over Remote Direct Memory Access (SMC-R) and Shared Memory Communications - Direct Memory Access (SMC-D), see Shared Memory Communications in z/OS Communications Server: IP Configuration Guide.

- **GetConnectionDetail (NWMTcpConnType)**

  Use this request to obtain information about active TCP connections, including SMC information for TCP connections that traverse SMC links.

  Guideline: When you use filters with this request, you can experience a performance improvement in retrieving the connection details if every filter contains a 4-tuple (local address, local port, remote address and remote port) for a connection. Additional filter values can be specified in each filter along with the 4-tuple.

- **GetDVIPAConnRTab (NWMDvConnRTabType)**

  Use this request to obtain information about dynamic virtual IP addresses (DVIPA) connections. This call returns a list of IPv4 and IPv6 DVIPA TCP connections. Entries are returned for the following:

  – All DVIPA interfaces for which MOVEABLE IMMEDIATE or NONDISRUPTIVE was specified.

  – On a sysplex distributor routing stack, every connection that is being routed through this distributor.

  – On a stack taking over a DVIPA, every connection to the DVIPA.

  – On a sysplex distributor target stack or a stack that is in the process of giving up a DVIPA, every connection for which the stack is an endpoint.

If none of these apply, then an empty response buffer is returned with a successful reason value, return code, and reason code. If the invoked TCP/IP stack has not joined a sysplex, then return value -1, return code EAGAIN, and reason code JRMustBeSysplex are returned without any other data.

- **GetDVIPAList (NWMDvListType)**

  Use this request to obtain information about dynamic virtual IP addresses (DVIPAs). This request returns a list of all IPv4 and IPv6 DVIPAs for the invoked TCP/IP stack. For each DVIPA, the MVS system name, TCP/IP job name, and various status information are returned.

- **GetDVIPAPortDist (NWMDvPortDistType)**

  Use this request to obtain information about dynamic virtual IP address (DVIPA) port distribution. This request returns a list of IPv4 and IPv6 distributed DVIPAs and ports. For each distributed DVIPA and port pair, one or more entries are returned for each target TCP/IP stack. If the invoked TCP/IP stack has not joined a sysplex, then return value -1, return code EAGAIN, and reason code JRMustBeSysplex are returned without any other data. If the TCP/IP stack is not a distributing stack, then an empty response buffer is returned with a successful return value, return code, and reason code. If the same DVIPA and port pair are affected by more than one QOS Policy, then an entry with the same DVIPA and port is returned for each QOS policy.

- **GetDVIPARoute (NWMDvRouteType)**

  Use this request to obtain information about dynamic virtual IP address (DVIPA) routes. This request returns a list of information that is defined on VIPAROUTE profile statements. Each entry includes the dynamic XCF address of a target TCP/IP stack and the corresponding target IP address that is used to route connection requests to that TCP/IP stack. Output is returned only by a distributing TCP/IP stack, or by a backup TCP/IP stack for a distributed DVIPA when the backup TCP/IP stack is assuming ownership of the distributed DVIPA. If the invoked TCP/IP stack has not joined a sysplex, then return value -1, return code EAGAIN, and reason code JRMustBeSysplex are returned without any other data. If the invoked TCP/IP stack is neither a distributing stack nor a backup stack, then an empty response buffer is returned with a successful return value, return code, and reason code.

- **GetFTPDaemonConfig (NWMFTPDConfigType)**

  Use this request to obtain configuration data from one active FTP daemon.

  Rules: You must supply only one filter when using this request type. If the filter number is not 1 in the request header, the following information is returned:

  – Return value -1
  – Return code EINVAL
  – Reason code JRInvalidValue

  The filter must contain the ASID of the specific FTP daemon for which you want to obtain the configuration data. If no ASID is specified in the filter, the following information is returned:

  – Return value -1
  – Return code EINVAL
  – Reason code JRInvalidFilter

  To obtain the ASID for the FTP daemon, take the following steps:

  – Invoke EZBNMIFR for the GetTCPListener request to each TCP/IP stack to obtain the active FTP daemons.

- Specify a filter with the application data (NWMFilterApplData) value of EZAFTP0D in the first 8 bytes to filter the active FTP daemons from other listeners. A daemon might be listening on multiple stacks.
- Extract the ASID (NWMTCPLAsid) of each FTP daemon returned by the GetTCPListener request for which the GetFTPDaemonConfig request is issued.
- Invoke EZBNMIFR for the GetFTPDaemonConfig request.
- Specify a filter that contains the ASID of the FTP daemon to obtain the configuration data of the FTP daemon.

- **GetGlobalStats (NWMGlobalStatsType)**

  Use this request to obtain TCP/IP stack global statistics for IP, ICMP, TCP, SMC, and UDP processing. The statistics that are returned by the request are similar to those in the output of the Netstat STATS/-S report. This request does not support filtering.

- **GetIfs (NWMIfsType)**

  Use this request to obtain TCP/IP stack interface attributes and IP addresses. The attributes and IP address information that are returned by the request are similar to those in the output of the Netstat DEVLINKS/-d and HOME/-h reports. Detailed attribute information is supported only for strategic interface types. The strategic interface types are:
  - Loopback
  - OSA-Express QDIO Ethernet
  - HiperSockets
  - Multipath Channel Point-to-Point
  - Static VIPA

  IBM 10GbE RoCE Express interfaces are also strategic interfaces. Some information about 10GbE RoCE Express interfaces is reported on this request, but the majority of the 10GbE RoCE Express attributes can be obtained from the GetRnics (NWMRnicType) NMI request.

  Internal shared memory (ISM) interfaces are also strategic interfaces. Some information about ISM interfaces is reported on this request, but the majority of the ISM attributes can be obtained from the GetIsms (NWMIsmType) NMI request.

  Dynamic VIPA interfaces are also strategic interfaces but their attributes can be obtained from the dynamic VIPA (DVIPA) NMI requests that are previously described in this topic. For non-strategic interface types, only the following information is provided:
  - Interface name from the LINK profile statement
  - Interface index
  - Associated device name from the DEVICE profile statement
  - Interface type
  - Interface status at the DEVICE and LINK level
  - Time stamp of last interface status change at the LINK level

  This request does not support filtering.

- **GetIfStats (NWMIfsStatsType)**

  Use this request to obtain TCP/IP stack interface statistics for all interface types except for 10GbE RoCE Express interfaces and ISM interfaces. The statistics that are returned by the request are similar to those in the output of the Netstat DEVLINKS/-d report with the addition of SNMP counters that are defined in the IF-MIB. For information about the IF-MIB, see RFC 2233. For information

about how to access RFCs, see Related protocol specifications. Statistics are provided for all strategic interface types except for VIPA interfaces; the stack does not maintain counters for VIPA interfaces. This request also provides a time stamp of when the counters were last reset. This request does not support filtering.

See GetRnics (NWMRnicType) NMI request for information about 10GbE RoCE Express interfaces. See GetIsms (NWMIsmType) NMI request for information about ISM interfaces.

- **GetIfStatsExtended (NWMIfsStatsExtType)**

  Use this request to obtain data link control (DLC) tuning statistics for datapath devices that are used by active OSA-Express QDIO Ethernet and HiperSockets interfaces. The statistics that are returned by the request are similar to those in the output of the VTAM TNSTATS function and the SMF type 50 record. Counters are provided for each read and write queue for each datapath device. Because of performance considerations, the counters are not maintained by default as part of TCP/IP stack initialization. The first GetIfStatsExtended request causes the counters to be maintained for all active interfaces. Therefore, the read and write queue counters can be 0 in the response for the first request.

  This request also provides a time stamp of when the counters were last reset. The counters are reset if all the interfaces that are using a datapath device are deactivated. This request does not support filtering.

- **GetIsms (NWMIsmType)**

  Use this request to obtain information about internal shared memory (ISM) interfaces. The ISM interface information that the request returns is similar to the information that is provided in the Netstat DEvlinks/-d report. This request also provides a time stamp of the last time when the ISM interface counters were reset. The values are reset if the ISM interface is deactivated. This request does not support filtering.

- **GetProfile (NWMProfileType)**

  Use this request to obtain information about the current TCP/IP profile statement settings. This request does not support filtering. To detect changes to the profile statement settings, callers can use this callable request to obtain an initial set of current profile settings, and then do one of the following actions:

  – Repeat the request, over a time interval, comparing returned data from a previous response to the returned data from the last response.

  – Obtain the SMF Type 119 subtype 4 TCP/IP profile event records. These records provide information about changes to the profile settings that are made by using the VARY TCPIP,,OBEYFILE command processing.

    - If the records are requested on the SMFCONFIG or NETMONITOR profile statements, they are created.
    - If the records are requested on the SMFCONFIG profile statement, they are written to the MVS SMF data sets.
    - If the records are requested on the NETMONITOR profile statement, they can be obtained from the real-time SMF data network management interface (NMI).

    For more information about the real-time SMF NMI, see Real-time TCP/IP network monitoring NMI. For more information about the TCP/IP profile SMF record, see “TCP/IP profile event record (subtype 4)” on page 181. The SMF record might be created even if some errors occurred during the VARY TCPIP,,OBEYFILE command processing. To determine whether profile

changes actually occurred, application programs that process these records must compare the sections of changed information to the previous profile settings.

- **GetRnics (NWMRnicType)**

  Use this request to obtain information about 10GbE RoCE Express interfaces.

  – The 10GbE RoCE Express interface information that the request returns is similar to the information that is provided in the Netstat DEvlinks/-d report.

  – The VTAM tuning statistics that the request returns are for active 10GbE RoCE Express interfaces only. These statistics are similar to those in the output of the VTAM TNSTAT function and the SMF type 50 record. Because of performance considerations, the counters are not maintained by default as part of VTAM or TCP/IP stack initialization. The first GetRnics request causes the counters to be maintained for all active 10GbE RoCE Express interfaces. Therefore, the counters can be 0 in the response for the first request.

  This request also provides a time stamp of the last time when the 10GbE RoCE Express interface counters and the VTAM tuning statistics were reset. The values are reset if the 10GbE RoCE Express interface is deactivated.

  This request does not support filtering.

- **GetSmcDLinks (NWMSmcDLinkType)**

  Use this request to obtain information about Shared Memory Communications - Direct Memory Access (SMC-D) links. The SMC-D link information that the request returns is similar to the information that is provided in the Netstat DEvlinks/-d report. This request does not support filtering.

- **GetSmcLinks (NWMSmcLinkType)**

  Use this request to obtain information about SMC-R link groups and the SMC-R links in each group. The SMC-R link group and SMC-R link information that is returned by the request is similar to the information provided in the Netstat DEvlinks/-d report. This request does not support filtering.

- **GetStorageStatistics (NWMStgStatsType)**

  Use this request to obtain information about TCP/IP storage utilization, including SMC storage utilization, and SMC-R send and receive buffer utilization. This request does not support filtering.

- **GetSysplexXCF (NWMSyXcfType)**

  Use this request to obtain information about all TCP/IP stacks in the subplex. This request returns a list of all TCP/IP stacks in the same subplex as the invoked TCP/IP stack. For each TCP/IP stack, the MVS system name and one or more dynamic XCF IP addresses are returned. There are no filters defined for this request. If the invoked TCP/IP stack has not joined a sysplex, then return value -1, return code EAGAIN, and reason code JRMustBeSysplex are returned without any other data.

- **GetTCPListeners (NWMTcpListenType)**

  Use this request to obtain information about active TCP listeners, including SMC information for TCP listeners that traverse SMC links.

- **GetTnConnectionData (NWMTnConnType)**

  Use this request to obtain information about TN3270E Telnet server connection performance data.

- **GetTnMonitorGroups (NWMTnMonGrpType)**

  Use this request to obtain information about TN3270E Telnet server monitor groups.

- **GetTnProfile (NWMTnProfileType)**

Use this request to obtain information about the current TN3270E Telnet server profile statement settings.

This request does not support filtering. To detect changes to the profile statement settings, callers can use this request to obtain an initial set of the current profile settings, and then do one of the following actions:

– Repeat the request, over a time interval, comparing returned data from a previous response to the returned data from the last response.
– Obtain the SMF Type 119 subtype 24 TN3270E Telnet server profile event records. These records provide information about changes to the profile settings that are made by using the VARY TCPIP,*tnproc*,OBEYFILE command processing.
  - If the records are requested by the TELNETGLOBALS SMFPROFILE profile statement or the TCP/IP stack NETMONITOR profile statement, they are created.
  - If the records are requested by the TELNETGLOBALS SMFCONFIG profile statement, they are written to the MVS SMF data sets.
  - If the records are requested by the NETMONITOR profile statement, they can be obtained from the real-time SMF data network management interface (NMI).

  For more information about the real-time SMF NMI, see Real-time TCP/IP network monitoring NMI. For more information about the TCP/IP profile SMF record, see TN3270E Telnet server profile event record (subtype 24). The SMF record might be created even if some errors occurred during the VARY TCPIP,*tnproc*,OBEYFILE command processing. To determine whether profile changes occurred, application programs that process these records must compare the sections of information in the new record with the previous profile settings.
– The NWMTnGrpDtl option flag allows the caller to obtain all the range data in the various groups that a Telnet profile defines. The call can return multiple entries and can use SMF119TN_*xx*RngNum to determine the number of ranges that are returned in each entry. If the flag is not set, the call returns one entry that contains only the first SMF119TN_*xx*RngMax ranges for a group. Based on the profile, specifying NWMTnGrpDtl can require a large amount of memory to hold the entire profile.

  Tip: Regardless of the number of entries that are returned for a group, the SMF119TN_*xx*RngCnt field indicates the total number of ranges that the group defines, and the SMF119TN_*xx*Count field indicates the total number of LUs or elements in the group.

- **GetUDPTable (NWMUdpConnType)**

  Use this request to obtain information about active UDP sockets.

The general format of the request consists of the request header and the request section descriptors (triplets), which define the input data. A triplet describes the input filters and contains the offset, in bytes, of the request section relative to the beginning of the request buffer, the number of elements in the request section, and the length of an element in the request section.

Filter request section

For requests that support filters, you can use filters to limit the data that is returned to data that matches the specified filter values. Not all filters are supported for all requests.

The following request types do not support any filters. If you specify filters for these requests, the filters are ignored.

- GetGlobalStats
- GetIfs
- GetIfStats
- GetIfStatsExtended
- GetIsms
- GetProfile
- GetRnics
- GetSmcLinks
- GetSmcDLinks
- GetStorageStatistics
- GetSysplexXCF
- GetTnMonitorGroups
- GetTnProfile

The following table describes all possible filters.

Table 5. Available EZBNMIFR poll-type request filters

Filter item	Filter item value
Application data	An EBCDIC character string (right-padded with blanks if less than 40 characters in length) associated with a TCP socket by the owning application using the SIOCSAPPLDATA IOCTL. The application data filter can have wildcard characters. Use a question mark (?) as a wildcard for a single character and an asterisk (*) as a wildcard for zero or more characters. For z/OS Communications Server applications, see Application data for applications that use the SIOCSAPPLDATA ioctl as a source for information about the content, format, and meaning of the application data that the applications associate with the sockets that they own. For other applications, see the documentation that is supplied by the application. See Miscellaneous programming interfaces for more information about associating application data with a socket.
Application name	An EBCDIC application name (right-padded with blanks if less than 8 characters in length) of the SNA application name in session with the TN3270E secondary LU representing the client. The application name can have wildcard characters. Use a question mark (?) as a wildcard for a single character, and an asterisk (*) as a wildcard for 0 or more characters. For example, the value A?C* matches all application names with a first character A and a third character C, but does not match 2-character names, names beginning with B through Z, or names with anything other than C in the third position.
ASID	A 16-bit address space number of a socket application address space.

Table 5. Available EZBNMIFR poll-type request filters (continued)

Filter item	Filter item value
Destination XCF IP address and family	A 32-bit IPv4 address or a 128-bit IPv6 address. The destination XCF IP address family field must also be set to indicate whether the destination XCF IP address filter value is an IPv4 address or an IPv6 address. For IPv4 addresses, the destination XCF IP address filter value can be specified as either an IPv4 address (for example, 9.1.2.3) or an IPv4-mapped IPv6 address (for example, ::FFFF:9.1.2.3). A null address can be specified as either an IPv4 address (0.0.0.0), an IPv4-mapped IPv6 address (::FFFF:0.0.0.0), or an IPv6 address (::). The destination XCF IP address family field must be set to AF_INET for an IPv4 address or AF_INET6 for an IPv6 address.
Destination XCF IP address prefix	A 16-bit signed binary value that specifies the number of destination XCF IP address bits to use. For example, the value 12 specifies that the first 12 bits of a destination XCF IP address are compared to the first 12 bits of the destination XCF IP address filter value. The value 0 specifies that all address bits are compared. A value greater than 32 for an IPv4 address, or greater than 128 for an IPv6 address, specifies that all address bits are compared.
Dynamic virtual IP address and family	A 32-bit IPv4 address or a 128-bit IPv6 address. The dynamic VIPA address family field must also be set to indicate whether the DVIPA filter value is an IPv4 address or an IPv6 address. For IPv4 addresses, the DVIPA filter value can be specified as either an IPv4 address (for example, 9.1.2.3) or an IPv4-mapped IPv6 address (for example, ::FFFF:9.1.2.3). A null address can be specified as either an IPv4 address (0.0.0.0), an IPv4-mapped IPv6 address (::FFFF:0.0.0.0), or an IPv6 address (::). The dynamic virtual IP address family field must be set to AF_INET for an IPv4 address or AF_INET6 for an IPv6 address.
Dynamic virtual IP address port	A 16-bit unsigned binary port number.
Dynamic virtual IP address prefix	A 16-bit signed binary value that specifies the number of dynamic virtual IP address bits to use. For example, the value 12 means that the first 12 bits of a dynamic VIPA are compared to the first 12 bits of the dynamic VIPA filter value. The value 0 means that all address bits are compared. A value greater than 32 for an IPv4 address, or greater than 128 for an IPv6 address, means that all address bits are compared.
Interface name	An EBCDIC interface name (right-padded with blanks if less than 16 characters in length) of an IPv4 or IPv6 interface. The interface name can have wildcard characters. Use a question mark (?) as a wildcard for a single character, and use an asterisk (*) as a wildcard for zero or more characters. For example, the value A?C* matches all interface names with a first character A and a third character C, but does not match 2-character names, names beginning with B through Z, or names that have anything other than the character C in the third position.

Table 5. Available EZBNMIFR poll-type request filters (continued)

Filter item	Filter item value
Local or source IP address	A 32-bit IPv4 address or a 128-bit IPv6 address. The local or source IP address filter value is specified as the IP address field within a sockaddr structure. The sockaddr address family field must be set to indicate whether the local IP address filter value is an IPv4 address or an IPv6 address. For IPv4 connections, the local IP address filter value can be specified as either an IPv4 address (for example, 9.1.2.3) or an IPv4-mapped IPv6 address (for example, ::FFFF:9.1.2.3). For all connections, a null address can be specified as either an IPv4 address (0.0.0.0), an IPv4-mapped IPv6 address (::FFFF:0.0.0.0), or an IPv6 address (::).
Local or source IP address prefix	A 16-bit signed binary value that specifies the number of local or source IP address bits to use. For example, the value 12 means that the first 12 bits of a local or source IP address are compared to the first 12 bits of the local IP address filter value. The value 0 means that all address bits are compared. A value greater than 32 for an IPv4 address, or greater than 128 for an IPv6 address, means that all address bits are compared.
Local or source port	A 16-bit unsigned binary port number.
LU name	An EBCDIC LU name (right-padded with blanks if less than 8 characters in length) of the TN3270E LU representing the client. Use a question mark (?) as a wildcard for a single character and an asterisk (*) as a wildcard for zero or more characters. For example, the value A?C* matches all names with a first character A and a third character C, but does not match 2-character names, names beginning with B through Z, or names with anything other than C in the third position.
Monitor group identifier	A 32-bit unsigned binary value assigned by the TN3270E Telnet server to identify up to 255 unique monitor groups. Any parameter change within an existing monitor group or a new monitor group causes the TN3270E Telnet server to assign a new identifier. The identifier is reported in the monitor group table and connection data allowing a comparison between monitoring criteria and actual connection performance. The monitor group identifier can be obtained by issuing the GetTnMonitorGroups request.
Remote or destination IP address	A 32-bit IPv4 address or a 128-bit IPv6 address. The remote or destination IP address filter value is specified as the IP address field within a sockaddr structure. The sockaddr address family field must be set to indicate whether the remote IP address filter value is an IPv4 address or an IPv6 address. For IPv4 connections, the remote IP address filter value can be specified as either an IPv4 address (for example, 9.1.2.3) or an IPv4-mapped IPv6 address (for example, ::FFFF:9.1.2.3). For all connections, a null address can be specified as either an IPv4 address (0.0.0.0), an IPv4-mapped IPv6 address (::FFFF:0.0.0.0), or an IPv6 address (::).
Remote or destination IP address prefix	A 16-bit signed binary value specifying the number of remote or destination IP address bits to use. For example, the value 12 means that the first 12 bits of a remote or destination IP address are compared to the first 12 bits of the remote IP address filter value. The value 0 means that all address bits are compared. A value greater than 32 for an IPv4 address, or greater than 128 for an IPv6 address, means that all address bits are compared.

Table 5. Available EZBNMIFR poll-type request filters (continued)

Filter item	Filter item value
Resource ID	A 32-bit unsigned binary TCP/IP resource identifier (`Client ID` in Netstat displays).
Resource name	An EBCDIC job name, right-padded with blanks if less than 8 characters long, of a socket application address space (`Client Name` in Netstat displays). A question mark can be used to wildcard a single character, and an asterisk can be used to wildcard zero or more characters. For example, the value A?C* matches all names with a first character A and a third character C, but does not match two-character names or names beginning with B through Z.
Remote or destination port	A 16-bit unsigned binary port number.
Server resource ID	A 32-bit unsigned binary TCP/IP resource identifier of the related server listening connection.
Target IP address and family	A 32-bit IPv4 address or a 128-bit IPv6 address. The target IP address family field must also be set to indicate whether the target IP address filter value is an IPv4 address or an IPv6 address. For IPv4 addresses, the destination XCF IP address filter value can be specified as either an IPv4 address (for example, 9.1.2.3) or as an IPv4-mapped IPv6 address (for example, ::FFFF:9.1.2.3). A null address can be specified as either an IPv4 address (0.0.0.0), as an IPv4-mapped IPv6 address (::FFFF:0.0.0.0), or as an IPv6 address (::). The target IP address family field must be set to AF_INET for an IPv4 address or AF_INET6 for an IPv6 address.
Target IP address prefix	A 16-bit signed binary value that specifies the number of target IP address bits to use. For example, the value 12 means that the first 12 bits of a target IP address are compared to the first 12 bits of the target IP address filter value. The value 0 means that all address bits are compared. A value greater than 32 for an IPv4 address, or greater than 128 for an IPv6 address, means that all address bits are compared.

You can specify 1 - 4 filter elements. Each filter element can contain any combination of the items that are listed in Table 5 on page 167. A filter element that does not have any applicable items matches all data for the request. The data must match all items that are specified in a filter element to pass that filter check; data must pass at least one filter check to be selected.

If you do not specify any filters (triplet offset field is 0, or triplet element count field is 0, or triplet element length field is 0), then the caller is requesting all information that is applicable to that request except for the GetFTPDaemonConfig request type.

The following list shows the applicable filter items that each request type supports. If you specify inapplicable filters for a particular request type, they are ignored.

- GetConnectionDetail
  - Application data
  - ASID
  - Local or source IP address
  - Local or source IP address prefix

  - Local or source port
  - Remote or destination IP address
  - Remote or destination IP address prefix
  - Remote or destination port
  - Resource ID
  - Resource name
  - Server resource ID
- GetDVIPAConnRTab
  - Destination XCF IP address and family
  - Destination XCF IP address prefix
  - Local or source IP address
  - Local or source IP address prefix
  - Local or source port
  - Remote or destination IP address
  - Remote or destination IP address prefix
  - Remote or destination port
- GetDVIPAList
  - Dynamic virtual IP address and family
  - Dynamic virtual IP address prefix
  - Interface name
- GetDVIPAPortDist
  - Destination XCF IP address and family
  - Destination XCF IP address prefix
  - Dynamic virtual IP address and family
  - Dynamic virtual IP address port
  - Dynamic virtual IP address prefix
- GetDVIPARoute
  - Destination XCF IP address and family
  - Destination XCF IP address prefix
  - Target IP address and family
  - Target IP address prefix
- GetFTPDaemonConfig
  - ASID of an FTP daemon address space.
- GetTCPListeners
  - Application data
  - ASID
  - Local or source IP address
  - Local or source IP address prefix
  - Local or source port
  - Resource ID
  - Resource name
- GetTnConnectionData
  - Application name
  - Local or source IP address
  - Local or source IP address prefix

  - Local or source port
  - LU name
  - Monitor group identifier
  - Remote or destination IP address
  - Remote or destination IP address prefix
  - Remote or destination port
  - Resource ID
  - Server resource ID
- GetUDPTable
  - ASID
  - Local or source IP address
  - Local or source IP address prefix
  - Local or source port
  - Resource ID
  - Resource name

TCP/IP NMI response format

The following list describes the general format of the response:

- The response header, which is defined by the NWMHeader structure, the request section descriptors (triplets), and the response section descriptors (quadruplets). Processing is slightly different for the request types (poll-type and action-type) as described in the following topics.
- The request sections.
- The response output. See the following topics about the poll-type and action-type response output for a description.

  Guideline: Some of the data in the response output uses data structures in a variable size. Do not rely on the documented size of the data structure for accessing data. You must use the length field of the response output section descriptors (triplets) to determine the correct size of each response.

  Tip: Connection elements for TN3270E Telnet server connection performance data are returned only if the connection is being monitored by a MonitorGroup that is mapped to the connection. See Connection monitoring mapping statement in z/OS Communications Server: IP Configuration Guide for details.

Processing poll-type request responses

The format of the response output depends on the specific request.

- The following requests return one or more response section elements of the same type.

Table 6. Poll-type request responses

Request	Response
GetConnectionDetail	NWMTCPConnEntry (assembler), NWMConnEntry (C/C++)
GetDVIPAConnRTab	NWMDvConnRTabEntry
GetDVIPAList	NWMDvListEntry
GetDVIPAPortDist	NWMDvPortDistEntry

Table 6. Poll-type request responses (continued)

Request	Response
GetDVIPARoute	NWMDvRouteEntry
GetIfStats	NWMIfStatsEntry
GetIsms	NWMIsmEntry
GetSmcDLinks	NWMSmcDLinkEntry
GetStorageStatistics	NWMStgStatEntry
GetSysplexXCF	NWMSyXcfEntry
GetTCPListeners	NWMTCPListenEntry
GetTnConnectionData	NWMTnConnEntry
GetTnMonitorGroups	NWMTnMonGrpEntry
GetUDPTable	NWMUDPConnEntry

- The following requests return one or more records. Each record begins with an NWMRecHeader structure that describes the record. See the specific request topics for a detailed description of the response output of each request.
  - GetFTPDaemonConfig
  - GetGlobalStats
  - GetIfs
  - GetIfStatsExtended
  - GetProfile
  - GetRnics
  - GetSmcLinks
  - GetTnProfile

The response output is described by the response section quadruplet in the NWMHeader structure. The quadruplet consists of the following fields:

- The offset, in bytes, of the first response section element or record. This offset is relative to the beginning of the response buffer.
- The number of elements in the response section or the number of records that are returned.
- The length of a response section element for requests that return one or more response section elements of the same type. For requests that return one or more records, the value of this field is 0. The NWMRecHeader structure for each returned record contains the actual length of each record.
- The total number of elements that passed the requested filter checks.

The response header contains the number of bytes required to contain all the requested data. When the return code is ENOBUFS, use this value to allocate a larger request/response buffer and reissue the request.

GetFTPDaemonConfig response format

For the GetFTPDaemonConfig request, the output is returned as one record. The response section quadruplet contains the following values:

- The offset, which is in the response buffer, of the output record.
- The length of each element. It is always 0.

- The number of elements that are returned is always 1, which indicates that only one record was returned.
- The number of elements that matched the filters is always 1, which indicates that one record was matched.

The output record consists of the following fields:

Record header
The record header is mapped by the NWMRecHeader structure and consists of the following fields:
- An EBCDIC identifier.
- The total length of the record.
- The number, which is always 3, of section descriptors that are included in this record. The section descriptors are mapped by the NWMTriple structure.

Section descriptor triplets
The following three section descriptors that describe the returned information for each section type are always included. For each section type, only one section is included.
- FTP daemon identification section
- FTP daemon general configuration section
- FTP daemon configuration data section

The sections of data that this request provides are identical to the corresponding sections in the SMF 119 subtype 71 record. See FTP daemon configuration record (subtype 71) for the layout of these sections:

FTP daemon identification section - SMF119FT_FD
This section provides information that identifies which FTP daemon this record is collected for.

FTP daemon general configuration section - SMF119FT_FDCF
This section provides configuration information for the statements whose value has a fixed length.

FTP daemon configuration data section - SMF119FT_FDCD
This section provides configuration information for the statements whose value has a variable length. This section is a set of entries with a variable length for each statement. Each entry contains the following fields:
- Total length of the entry.
- Key of the entry. This value identifies the statement that the entry represents.
- Value that is specified for the statement.

In this section, only statements that are explicitly specified or have default values are provided. You can use the SMF119FT_FDCD_Key value of each configuration data entry in this section to determine which statements are contained.

GetGlobalStats response format

For the GetGlobalStats request, the output is returned as one record. The response section quadruplet contains the following values:
- The offset, which is in the response buffer, of the output record.
- The length of each element. It is always 0.

- The number of elements in the response section. It is set to 1 to indicate that only one record was returned.
- The total number of matching elements. It is set to 1 because filters are not supported.

The output record consists of the following fields:

- Record header. The record header is mapped by the NWMRecHeader structure and consists of the following fields:
  - An EBCDIC identifier
  - The total length of the record
  - The number of section descriptors (mapped by the NWMTriple structure) that are present in this record
- Section descriptor triplets for each set of statistic counters. The returned statistic counters are similar to the counters in the output of the Netstat STATS/-S report. See Netstat STATS/-S report in z/OS Communications Server: IP System Administrator's Commands for a description of each field. The following section descriptors that describe the returned information for each section type are always included:
  - IP counters section - A section for IPv4 counters is always returned. If the TCP/IP stack is IPv6-enabled, a section for IPv6 counters is also returned.
  - IP general counters section - Only one section of this type is included.
  - TCP counters section - Only one section of this type is included. If Shared Memory Communications over Remote Direct Memory Access (SMC-R) was ever configured, this section includes SMC-R statistics. If SMC-D was ever configured, this section includes SMC-D statistics.
  - UDP counters section - Only one section of this type is included.
  - ICMP global counters section - A section for IPv4 counters is always returned. If the TCP/IP stack is IPv6-enabled, a section for IPv6 counters is also returned.
  - ICMP type counters section - One section is returned for each ICMP and ICMPv6 type. For more information about these types, see http://www.iana.org/assignments/icmp-parameters and http://www.iana.org/assignments/icmpv6-parameters.
- IP counters sections (NWMIpStatsEntry) - Sections for IPv4 and IPv6 counters.
- IP general counters section (NWMIpGenStatsEntry)
- TCP and SMC counters section (NWMTcpStatsEntry)
- UDP counters section (NWMUdpStatsEntry)
- ICMP global counters sections (NWMIcmpStatsEntry)
- ICMP type counters sections (NWMIcmpTypeStatsEntry)

GetIfs response format

For the GetIfs request, the output is returned as one record per interface. The response section quadruplet contains the following values:

- The offset, which is in the response buffer, of the first output record.
- The length of each element. It is always 0.
- The number of elements in the response section. It is set to the total number of records that are returned.
- The total number of matching elements. It is set to the number of records that are returned because filters are not supported.

All fields that contain EBCDIC values are padded with EBCDIC blanks (x'40') and are set to EBCDIC blanks if the field does not contain a value.

Each output record consists of the following fields:

- Record header. The record header is mapped by the NWMRecHeader structure and consists of the following fields:
  - An EBCDIC identifier
  - The total length of the record
  - The number of section descriptors (mapped by the NWMTriple structure) that are present in this record
- Section descriptor triplets. Two section descriptors that describe the returned information for each section type are always included:
  - Base section - Only one section of this type is included per interface.
  - IP address section - Only one section of this type is included for every IP address for the interface. If an interface does not have an IP address, the section descriptor triplet fields are all set to 0.
- Base section (NWMIfEntry). This section provides the interface name, status, and attributes.
- One or more IP address sections (NWMIpadEntry)

GetIfStatsExtended response format

For the GetIfStatsExtended request, the data link control (DLC) tuning statistics output is returned as one record per data subchannel address that is used by an OSA-Express QDIO ethernet or HiperSockets interface. The response section quadruplet contains the following values:

- The offset, which is in the response buffer, of the first output record.
- The length of each element. It is always 0.
- The number of elements in the response section. It is set to the total number of records that are returned.
- The total number of matching elements. It is set to the number of records that are returned because filters are not supported.

All fields that contain EBCDIC values are padded with EBCDIC blanks (x'40').

Each output record consists of the following fields:

- Record header. The record header is mapped by the NWMRecHeader structure and consists of the following fields:
  - An EBCDIC identifier
  - The total length of the record
  - The number of section descriptors (mapped by the NWMTriple structure) that are present in this record
- Section descriptor triplets. Four section descriptors that describe the information that is returned for each section type are always included:
  - Base section - Only one section of this type is included per data subchannel address.
  - Interface section - One section of this type is included for each interface that shares the data subchannel address.
  - Read queue counters section - There is one of these sections for the Primary read queue.per read queue supported for the data subchannel address. For more information about the OSA-Express read queues, see QDIO inbound

workload queueing in z/OS Communications Server: IP Configuration Guide. HiperSockets interfaces support only one read queue.

  - Write queue counters section - One section of this type is included for each of one to four possible write priority queues that are supported for the data subchannel address.

- Base section (NWMIFStExtBaseEntry). This section provides information about the data, read control, write control subchannel addresses, the TRLE name, and OSA-Express ports. This section also includes a time stamp of when the counters were last reset.
- Interface section (NWMIFStExtIntfEntry)
- Read queue sections (NWMIfStExtReadEntry)
- Write queue sections (NWMIfStExtWriteEntry)

GetProfile response format

For the GetProfile request, the output is returned as one record. The response section quadruplet contains the following values:

- Offset is the offset, into the response buffer, of a GetProfile record header.
- The length of each element is always 0.
- The number of elements in the response section is always 1 to indicate that only one record was returned.
- The total number of matching elements is always 1, because filters are not supported.

The record header is mapped by the NWMRecHeader structure. The header consists of the following fields:

- An EBCDIC identifier
- The total length of the record
- The number of section descriptors (triplets) that are present in this record. Twenty-one section descriptors are always returned. The section descriptor triplets are mapped by the NWMTriple structure.

The section descriptors (triplets) immediately follow the record header, and the sections immediately follow the section descriptors. If there is no profile information for a section, the section descriptor triplet fields for that section all contain 0.

The section structures in the GetProfile response are identical to the section structures in the TCP/IP profile SMF 119 subtype 4 event records. If you already have an application that processes the SMF record section structures, you can also use it for processing the GetProfile response section structures. See “TCP/IP profile event record (subtype 4)” on page 181 for a layout of this SMF record.

In the GetProfile response, the Profile Information Common and Data Set Name sections primarily contain information about the initial profile, not about the last change to the profile; however, the following fields contain the date and time of the last change to the profile:

- NMTP_PICOChangeTime
- NMTP_PICOChangeDate

GetRnics response format

For the GetRnics request, the output is returned as one record per interface. The response section quadruplet contains the following values:

- The offset, which is in the response buffer, of the output record.
- The length of each element. It is always 0.
- The number of elements in the response section. It is set to the number of records that are returned.
- The total number of matching elements. It is set to the number of records that are returned because filters are not supported on the GetRnics request.

All fields that contain EBCDIC values are padded with EBCDIC blanks (X'40').

Each output record consists of the following fields:

- Record header. The record header is mapped by the NWMRecHeader structure and consists of the following fields:
  - An EBCDIC identifier
  - The total length of the record
  - The number of section descriptors (mapped by the NWMTriple structure) that are present in this record
- Section descriptor triplets. Two section descriptors that describe the returned information for each section type are always included:
  - Base 10GbE RoCE Express interface section; only one section of this type is included per interface.
  - VTAM tuning statistics section; only one section of this type is included per interface.
- Base 10GbE RoCE Express interface section (NWMRnicBaseEntry). This section provides the interface name, status, and attributes.
- VTAM tuning statistics section (NWMRnicTuningEntry). This section provides the VTAM tuning statistics information.

GetSmcLinks response format

For the GetSmcLinks request, the output is returned as one record per SMC-R link group. The response section quadruplet contains the following values:

- The offset, which is in the response buffer, of the output record.
- The length of each element. It is always 0.
- The number of elements in the response section. It is set to the number of records that are returned.
- The total number of matching elements. It is set to the number of records that are returned because filters are not supported on the GetSmcLinks request.

All fields that contain EBCDIC values are padded with EBCDIC blanks (X'40').

Each output record consists of the following fields:

- Record header. The record header is mapped by the NWMRecHeader structure and consists of the following fields:
  - An EBCDIC identifier
  - The total length of the record
  - The number of section descriptors (mapped by the NWMTriple structure) that are present in this record

- Section descriptor triplets. Two section descriptors that describe the returned information for each section type are always included:
  - SMC-R link group section; only one section of this type is included per SMC-R link group.
  - SMC-R link section; one section of this type is included for every SMC-R link that is a member of an SMC-R link group.
- SMC-R link group section (NWMSmcGrpEntry). This section provides the SMC-R link group identifier and statistics related to the SMC-R link group.
- SMC-R link section (NWMSmcLnkEntry). This section provides the SMC-R link local and remote identifiers and additional statistics related to the individual link.

GetTnProfile response format

For the GetTnProfile request, the output is returned as one record. The response section quadruplet contains the following values:

- Offset is the offset, into the response buffer, of a GetTnProfile record header.
- The length of each element is always 0.
- The number of elements in the response section is always 1 to indicate that only one record was returned.
- The total number of matching elements is always 1 because filters are not supported.

The NWMRecHeader structure maps the record header. The header consists of the following fields:

- An EBCDIC identifier.
- The total length of the record.
- The number of section descriptors (triplets) that are present in this record. Management section descriptors are always returned. The NWMTriple structure maps the section descriptors.

The section descriptors immediately follow the record header, and the sections immediately follow the section descriptors. If no profile information for a section is available, the section descriptor fields for that section are all 0.

The section structures in the GetTnProfile response are identical to the section structures in the TN3270E Telnet server profile SMF 119 subtype 24 event records. If you have an application that processes the SMF record section structures, you can use it to process the GetTnProfile response section structures. See TN3270E Telnet server profile event record (subtype 24) for a layout of this SMF record.

In the GetTnProfile response, the Profile Information and Data Set Name sections contain information about the last profile. The following fields contain the date and time when the last profile was activated:

- SMF119TN_PIProfStck
- SMF119TN_PIProfTime
- SMF119TN_PIProfDate

If the NWMTnGrpDtl flag is set, multiple entries for a group are generated. If the flag is not set, only the first entry of each group is available.

Processing action-type request responses

Processing the response for the DropConnection action-type request is described in this section.

For this type of request, the quadruplet contains the offset and number of elements, which is the same as the offset and number of elements in the triplet (output is the same as the input). If the call to EZBNMIFR returns a nonnegative return value, and the value for NWMQMatch returned in the quadruplet section is equal to the number of entries input, NWMQNumber, then all of the connections or endpoints were dropped successfully. If the call to EZBNMIFR returns a nonnegative return value, and if NWMQMatch is less than NWMQNumber, then not all of the connections or endpoints were successfully dropped. In this case, the program should examine the return code that is set in each NWMDropConnEntry field. If the value of the return code is nonzero, then this connection was not dropped; if the value of the return code is 0, then the connection was dropped.

The following describes the codes:

Table 7. Return code values

NWMDropConnRC	NWMDropConnRSN	Description
ENOENT	JRGetConnErr	The connection was not in the correct state for retrieving or the connection was not found.
EMVSERR	JRPATDELErr	Deletion of a restricted port entry failed.
EACCES	JRPORTACCESSAUTH	User does not have authority to access this port.
EMVSERR	JRPATFNDErr	Search for a restricted port failed or the connection was not found.
ENOENT	JRPATFNDErr	Search for a restricted port failed or the connection was not found.
ENOENT	JRGETCONNERR	The connection was not in the correct state for retrieving.
EAGAIN	JRUDPNOTUP	TCP/IP was not initialized
EAGAIN	JRTCPNOTUP	The request was not successful. The target TCP/IP stack was not active.
EINVAL	JRINVALIDVALUE	The request was not successful. A value that is not valid was specified in the request/response header.

Guideline: Input to the DropConnection request will most likely be from the output result of a GetUDPTable or GetConnectionDetail request where the filtered connection information might return connections that are not intended for termination. Applications that support the DropConnection request should be

coded to ensure that the connections input for termination have been examined carefully by programming logic that selects connections that meet a specific criteria, such as state.

Example

One NWMDropConnEntry is submitted:

```
Resource ID =003A, Local IP Address=9.0.0.1, Local Port=5003,
Remote IP Address=9.0.0.5, Remote Port=3000, Protocol=TCP
```

The following TCP connections exist:

- Resource Name = FTP1, Resource ID = 001A, Local IP Address = 9.0.0.2, Local Port = 5000,Remote IP Address = 9.0.0.5, Remote Port = 3001
- Resource Name = FTP2, Resource ID = 002A, Local IP Address = 9.0.0.1, Local Port = 5001,Remote IP Address = 9.0.0.5, Remote Port = 3002
- Resource Name = USR1, Resource ID = 004F, Local IP Address = 9.0.0.1, Local Port = 5002,Remote IP Address = 9.0.0.5, Remote Port = 3003
- Resource Name = USR7, Resource ID = 003A, Local IP Address = 9.0.0.1, Local Port = 5003, Remote IP Address = 9.0.0.5, Remote Port = 3000

When a DropConnection request is made, connection 4 is dropped because it matches the five required items.

TCP/IP profile event record (subtype 4)

The TCP/IP profile record provides profile information for the TCP/IP stack. The first or only record always contains the following sections:

- SMF header
- Self-defining section with 21 section triplets
- TCP/IP identification section
- Profile information common section
- Profile information data set name section

See TCP/IP profile record self-defining section for a list of all the sections of information that can be provided in this SMF record.

This record is created as an event record during the following processing:

- During the initialization of the stack. In this case, the record contains the complete profile information for the stack.
- If the profile is changed by the use of the VARY TCPIP,,OBEYFILE command. In this case, the record contains only changed profile information.
- The NMTP_PICOSecChanged flag bits in the profile information common section indicate which sections actually contain changed information.
- In the self-defining section, the triplet field values are zero for sections for which no information was changed, or for those sections which all the information was deleted from the stack's configuration.
- If deprecated profile statements were specified in the VARY TCPIP,,OBEYFILE command data set, field NMTP_PicoDepChanged indicates which statements were processed. If only deprecated statements were processed, the profile information common and data set name sections are the only sections of information provided in the SMF record. See Profile information common section for an explanation of deprecated profile statements.

- For the sections that changed, the section in the SMF record contains all of the information for the section. For example, if a network interface was added, the whole interface section is included in the SMF record. Applications need to compare the interface section in the new record with the interface section in the previous record to determine which interface was added.
- If the profile data set referenced by the VARY TCPIP,,OBEYFILE command changed the SMFCONFIG setting from PROFILE to NOPROFILE, one final SMF event record is created and written to the MVS SMF data sets to record this change.
- If the profile data set referenced by the VARY TCPIP,,OBEYFILE command changed the NETMONITOR SMFSERVICE setting from PROFILE to NOPROFILE, one final SMF event record is created and written to the real-time SMF data network management interface (NMI) to record this change. For more information about the real-time SMF NMI, see Real-time TCP/IP network monitoring NMI.

The SMF record might be created even if some errors occurred during processing the VARY TCPIP,,OBEYFILE command. Application programs that process these records must compare the sections of changed information to the previous profile settings to determine if profile changes actually occurred.

TCP/IP profile record IPv4 configuration section

This section provides IPv4 layer configuration information from the IPCONFIG, ARPAGE, and PRIMARYINTERFACE profile statements. There is only one of these sections in the record.

Table 8 shows the IPv4 configuration section.

Table 8. IPv4 configuration section

Offset	Name	Length	Format	Description
0(X'0')	NMTP_V4CFEye	4	EBCDIC	V4CF eyecatcher

Table 8. IPv4 configuration section (continued)

Offset	Name	Length	Format	Description
4(X'4')	NMTP_V4CFFlags	4	Binary	IPCONFIG flags: **X'80000000'** NMTP_V4CFCLAWDblNoop: If set, the CLAW channel programs have 2 NOP CCWs at the end. **X'40000000'** NMTP_V4CFDatagramFwd: If set, the stack is forwarding datagrams and field NMTP_V4CFFwdMultipPkt indicates if a multipath per packet algorithm is being used for forwarded packets. If not set, the stack is not forwarding datagrams. **X'20000000'** NMTP_V4CFFwdMultipPkt: This flag is valid only if flag NMTP_V4CFDatagramFwd is set. If the NMTP_V4CFFwdMultipPkt flag is set, the stack is forwarding datagrams using a multipath per packet algorithm. If not set, the stack is not using a multipath algorithm when forwarding datagrams. **X'10000000'** NMTP_V4CFDynamicXcf: If set, dynamic XCF interfaces are defined and the following fields contain dynamic XCF configured values: • NMTP_V4CFDynXcfAddr • NMTP_V4CFDynXcfCostMetric • NMTP_V4CFDynXcfMask • NMTP_V4CFDynXcfSecClass • NMTP_V4CFDynXcfSMCD

Table 8. IPv4 configuration section (continued)

Offset	Name	Length	Format	Description
4(X'4') (Cont)				**X'08000000'** NMTP_V4CFFormatLong: If set, the Netstat command displays the report output in long format. This flag is always set for IPv6-enabled stacks. **X'04000000'** NMTP_ V4CFIgnoreRedirectCfg: If set, IGNOREREDIRECT was specified on the IPCONFIG profile statement. **X'02000000'** NMTP_ V4CFIgnoreRedirectAct: If set, the stack is ignoring ICMP redirects and the NMTP_V4CFIgnRedirectRsn field indicates the reason why this setting is in effect. **X'01000000'** NMTP_V4CFIPSecurity: If set, IP security is enabled. **X'00800000'** NMTP_V4CFIQDIORouting: If set, IQDIO routing is enabled. **X'0040000'** NMTP_V4CFMultipPerConn: If set, the stack is using a multipath per connection routing selection algorithm for outbound IP traffic. **X'0020000'** NMTP_V4CFMultipPerPkt: If set, the stack is using a multipath per packet routing selection algorithm for outbound IP traffic. **X'00100000'** NMTP_V4CFPathMtuDisc: If set, Path MTU discovery is in effect. **X'00080000'** NMTP_V4CFSourceVipa: If set, the stack uses the appropriate VIPA IP address as the source IP address for outbound packets.

Table 8. IPv4 configuration section (continued)

Offset	Name	Length	Format	Description
4(X'4') (Cont)				**X'00040000'** NMTP_V4CFStopClawErr: If set, the stack stops channel programs when a CLAW error is detected. **X'00020000'** NMTP_V4CFSysplexRouting: If set, the stack communicates interface changes to the workload manager. **X'00010000'** NMTP_V4CFTCPSourceVipa: If set, and NMTP_V4CFSourceVipa is also set, the stack uses the address in field V4CFTcpSrcVipaAddr as the source IP address for outbound TCP connections. **X'00008000'** NMTP_V4CFQDIOAcc: If set, the QDIO accelerator function is enabled. **X'00004000'** NMTP_V4CFChkOffload: If set, IP, UDP and TCP checksum processing is offloaded to an OSA-Express feature. **X'00002000'** NMTP_V4CFSegOffload: If set, TCP segmentation is offloaded to an OSA-Express feature. **X'00001000'** NMTP_V4CFDynXcfSrcVipaIfNameFlg: If set, the NMTP_V4CFDynXcfSrcVipaIfName field contains the specified source VIPA interface name. **X'00000800'** NMTP_V4CFDynXcfSMCD: If set, the dynamically generated XCF interface can be used for new TCP connections with SMC-D.
8(X'8')	NMTP_V4CFArpTimeout	4	Binary	ARP cache timeout in seconds. If the value was configured, then it was either specified on the ARPAGE statement, or on the ARPTO parameter of the IPCONFIG statement.
12(X'C')	NMTP_V4CFDevRetry	4	Binary	Device retry duration in seconds
16(X'10')	NMTP_V4CFTcpSrcVipaAddr	4	Binary	VIPA source IP address for outbound TCP connections. If flags NMTP_V4CFSourceVipa and NMTP_V4CFTCPSourceVipa are set, this address is used as the source IP address.
20(X'14')	NMTP_V4CFDynXcfAddr	4	Binary	Dynamic XCF IP address. This field is valid only if the NMTP_V4CFDynamicXcf flag is set.
24(X'18')	NMTP_V4CFDynXcfCostMetric	1	Binary	Dynamic XCF cost metric. This field is valid only if the NMTP_V4CFDynamicXcf flag is set.

Table 8. IPv4 configuration section (continued)

Offset	Name	Length	Format	Description
25(X'19')	NMTP_V4CFDynXcfMask	1	Binary	Dynamic XCF number of mask bits. This field is valid only if the NMTP_V4CFDynamicXcf flag is set.
26(X'1A')	NMTP_V4CFDynXcfSecClass	1	Binary	Dynamic XCF security class. This field is valid only if the NMTP_V4CFDynamicXcf flag is set.
27(X'1B')	NMTP_V4CFQDIOPriority	1	Binary	IQDIO routing priority. This field is valid only if either the NMTP_IQDIORouting flag or the NMTP_QDIOAcc flag is set.
28(X'1C')	NMTP_V4CFIgnRedirectRsn	1	Binary	For one of the following reasons is why the NMTP_ V4CFIgnoreRedirectAct flag is set: • NMTP_V4CFIgnRedRsn_CFG(1) - Set by configuration • NMTP_V4CFIgnRedRsn_OMP(2) - Set due to OMPROUTE • NMTP_V4CFIgnRedRsn_IDS(3) - Set due to IDS ICMP redirect policy This field is valid only if the NMTP_ V4CFIgnoreRedirectAct flag is set.
29(X'1D')	NMTP_V4CFReasmTimeout	1	Binary	Reassembly timeout in seconds
30(X'1E')	NMTP_V4CFTTL	1	Binary	Time to live
31(X'1F')		1	Binary	Reserved
32(X'20')	NMTP_V4CFPrimaryIntfName	16	EBCDIC	Name of the primary interface. The primary interface could have been configured on a PRIMARYINTERFACE profile statement, or the stack could have selected a default primary interface.
48(X'30')	NMTP_V4CFDynXcfSrcVipaIfName	16	EBCDIC	Dynamic XCF source VIPA interface name. This field is valid only if the NMTP_V4CFDynXcfSrcVipaIfNameFlg flag is set.

TCP/IP profile record IPv6 configuration section

This section provides IPv6 layer configuration information from the IPCONFIG6 profile statement. There is only one of these sections in the record.

Table 9 shows the IPv6 configuration section.

Table 9. TCP/IP profile record IPv6 configuration section

Offset	Name	Length	Format	Description
0(X'0')	NMTP_V6CFEye	4	EBCDIC	V6CF eyecatcher

Table 9. TCP/IP profile record IPv6 configuration section (continued)

Offset	Name	Length	Format	Description
4(X'4')	NMTP_V6CFFlags	4	Binary	IPCONFIG6 Flags: **X'80000000', NMTP_V6CFDatagramFwd:** If set, the stack is forwarding datagrams and field NMTP_V6CFFwdMultipPkt indicates if a multipath per packet algorithm is being used for forwarded packets. If not set, the stack is not forwarding datagrams **X'40000000', NMTP_V6CFFwdMultipPkt:** This flag is valid only if flag NMTP_V6CFDatagramFwd is set. If the NMTP_V6CFFwdMultipPkt flag is set, the stack is forwarding datagrams using a multipath per packet algorithm. If not set, the stack is not using a multipath algorithm when forwarding datagrams. **X'20000000', NMTP_V6CFDynamicXcf** If set, dynamic XCF interfaces are defined and the following fields contain dynamic XCF configured values: • NMTP_V6CFDynXcfAddr • NMTP_V6CFDynXcfPfxRteLen • NMTP_V6CFDynXcfSecClass • NMTP_V6CFDynXcfSMCD **X'10000000', NMTP_V6CFDynXcfIntfIDFlg:** If set, field NMTP_V6CFDynXcfIntfID contains the specified interface ID value. **X'08000000', NMTP_V6CFDynXcfSrcVipaIfNameFlg:** If set, field NMTP_V6CFDynXcfSrcVipaIfName contains the specified source VIPA interface name. **X'04000000', NMTP_ V6CFIgnoreRedirectCfg:** If set, IGNOREREDIRECT was specified on the IPCONFIG6 profile statement. **X'02000000', NMTP_ V6CFIgnoreRedirectAct:** If set, the stack is ignoring ICMPv6 redirects and the NMTP_V6CFIgnRedirectRsn field indicates the reason why this setting is in effect **X'01000000', NMTP_ V6CFIgnoreRtrHopLimit:** If set, the stack is ignoring hop limits received in router advertisements.

Table 9. TCP/IP profile record IPv6 configuration section (continued)

Offset	Name	Length	Format	Description
4(X'4') (Cont)				**X'00800000', NMTP_V6CFIPSecurity:** If set, IP security is enabled. **X'00400000', NMTP_V6CFMultipPerConn:** If set, the stack is using a multipath per connection routing selection algorithm for outbound IP traffic. **X'00200000', NMTP_V6CFMultipPerPkt:** If set, the stack is using a multipath per packet routing selection algorithm for outbound IP traffic. **X'00100000', NMTP_V6CFSourceVipa:** If set, the TCP/IP stack uses the appropriate VIPA IP address as the source IP address for outbound packets **X'00080000', NMTP_V6CFTCPSourceVipa:** If set, and NMTP_V6CFSourceVipa is also set, the stack uses the interface in field V6CFTcpSrcVipaIntfName to determine the source IP address for outbound TCP connections. **X'00040000', NMTP_V6CFTempAddrs:** If set, the TCP/IP stack generates IPv6 temporary addresses for IPAQENET6 OSA-Express QDIO interfaces for which stateless address autoconfiguration is enabled. When this flag is set, the following fields contain life time values for the generated addresses: • NMTP_V6CFTempAddrsPrefLifeTime • NMTP_V6CFTempAddrsValidLifeTime **X'00020000'** NMTP_V6CFChkOffload: If set, UDP and TCP checksum processing is offloaded to an OSA-Express feature. **X'00010000'** NMTP_V6CFSegOffload: If set, TCP segmentation is offloaded to an OSA-Express feature. **X'00008000'** NMTP_V6CFDynXcfSMCD: If set, the dynamically generated XCF interface can be used for new TCP connections with SMC-D.
8(X'8')	NMTP_V6CFDynXcfIntfID	8	Binary	Dynamic XCF interface ID. This field is valid only if the NMTP_V6CFDynXcfIntfIDFlg flag is set.
16(X'10')	NMTP_V6CFDynXcfAddr	16	Binary	Dynamic XCF IP address. This field is valid only if the NMTP_V6CFDynamicXcf flag is set.
32(X'20')	NMTP_V6CFDynXcfSrcVipaIntfName	16	EBCDIC	Dynamic XCF source VIPA interface name. This field is valid only if the NMTP_V6CFDynXcfSrcVipaIfNameFlg flag is set.
48(X'30')	NMTP_V6CFTcpSrcVipaIntfName	16	EBCDIC	The VIPA interface name that is used for source IP address selection for outbound TCP connections. This field is valid only if flags NMTP_V6CFSourceVipa and NMTP_V6CFTCPSourceVipa are set.

Table 9. TCP/IP profile record IPv6 configuration section (continued)

Offset	Name	Length	Format	Description
64(X'40')	NMTP_V6CFDynXcfPfxRteLen	1	Binary	Dynamic XCF prefix route length. This field is valid only if the NMTP_V6CFDynamicXcf flag is set. If a prefix route length was not specified, then the value is zero.
65(X'41')	NMTP_V6CFDynXcfSecClass	1	Binary	Dynamic XCF security class. This field is valid only if the NMTP_V6CFDynamicXcf flag is set.
66(X'42')	NMTP_V6CFHopLimit	1	Binary	Hop limit for outbound packets.
67(X'43')	NMTP_V6CFIcmpErrLimit	1	Binary	Number of ICMPv6 error messages sent per second to a particular IPv6 destination.
68(X'44')	NMTP_V6CFIgnRedirectRsn	1	Binary	The following are reasons that the NMTP_ V6CFIgnoreRedirectAct flag is set: • NMTP_V6CFIgnRedRsn_CFG(1) - Set by configuration • NMTP_V6CFIgnRedRsn_OMP(2) - Set due to OMPROUTE • NMTP_V6CFIgnRedRsn_IDS(3) - Set due to IDS ICMPv6 redirect policy This field is valid only if the NMTP_ V6CFIgnoreRedirectAct flag is set.
69(X'45')	NMTP_V6CFOSMSecClass	1	Binary	OSM security class. This field is valid only when flag NMTP_V6CFIPSecurity is set.
70(X'46')		2	Binary	Reserved
72(X'48')	NMTP_V6CFTempAddrsPrefLifeTime	2	Binary	Preferred life time for temporary addresses, specified in hours. This field is valid only if the NMTP_V6CFTempAddrs flag is set.
74(X'4A')	NMTP_V6CFTempAddrsValidLifeTime	2	Binary	Valid life time for temporary addresses, specified in hours. This field is valid only if the NMTP_V6CFTempAddrs flag is set.

TCP/IP profile record Global configuration section

This section provides Global configuration information from the GLOBALCONFIG profile statement. There is only one of these sections in the record.

Table 10 shows the TCP/IP profile record Global configuration section.

Table 10. TCP/IP profile record Global configuration section

Offset	Name	Length	Format	Description
0(X'0')	NMTP_GBCFEye	4	EBCDIC	GBCF eyecatcher

Table 10. TCP/IP profile record Global configuration section (continued)

Offset	Name	Length	Format	Description
4(X'4')	NMTP_GBCFFlags	2	Binary	Flags: **X'8000', NMTP_GBCFExpBindPortRange:** If set, fields NMTP_GBCFExpBindPortRangeBegNum and NMTP_GBCFExpBindPortRangeEndNum contain the beginning and ending port numbers of the range of reserved TCP ports in the sysplex. **X'4000', NMTP_GBCFIqdMultiWrite:** If set, multiple write support is enabled for HiperSockets interfaces. **X'2000', NMTP_GBCFMlsCheckTerminate:** If set, the stack terminates if multi-level secure configuration inconsistencies are encountered. **X'1000', NMTP_GBCFSegOffload:** If set, TCP segmentation is offloaded to an OSA-Express feature. **Guideline:** This flag is deprecated. Use NMTP_V4CFSegOffload instead. **X'0800', NMTP_GBCFTcpipStats:** If set, several counters are written to the CFGPRINT DD data set when the TCP/IP stack terminates. **X'0400', NMTP_GBCFZiip:** If set, field NMTP_GBCFZiipOptions indicates for which workloads CPU cycles are displaced to a zIIP. **X'0200', NMTP_GBCFWlmPriorityQ:** If set, the following fields indicate the OSA-Express QDIO priority values that are assigned for packets associated with WLM service classes and for forwarded packets according to the control values for the WLMPRIORITYQ parameter: • NMTP_GBCFWPQCV0Pri • NMTP_GBCFWPQCV1Pri • NMTP_GBCFWPQCV2Pri • NMTP_GBCFWPQCV3Pri • NMTP_GBCFWPQCV4Pri • NMTP_GBCFWPQCV5Pri • NMTP_GBCFWPQCV6Pri • NMTP_GBCFWPQFwdPri **X'0100', NMTP_GBCFSMCR:** If set, this stack is enabled for SMC-R communications. **X'0080', NMTP_GBCFSMCD:** If set, this stack is enabled for SMC-D communications.

Table 10. TCP/IP profile record Global configuration section (continued)

Offset	Name	Length	Format	Description
6(X'6')	NMTP_GBCFSysMonOptions	2	Binary	The following are sysplex monitor subparameter settings: **X'8000', NMTP_GBCFSysMonAutoRejoin:** If set, the stack automatically rejoins the sysplex group after problems that caused it to leave the sysplex group are resolved. **X'4000', NMTP_GBCFSysMonDelayJoin:** If set, the stack delays joining the sysplex group until OMPROUTE is active. **X'2000', NMTP_GBCFSysMonDynRoute:** If set, the TCP/IP stack monitors the presence of dynamic routes over those network interfaces for which the MONSYSPLEX parameter was specified. This setting is dynamically changed if the MONINTERFACE or NOMONINTERFACE subparameters are specified. **X'1000', NMTP_GBCFSysMonMonIntf:** If set, the TCP/IP stack monitors the status of network interfaces for which the MONSYSPLEX parameter was specified. **X'0800', NMTP_GBCFSysMonRecovery:** If set, the TCP/IP stack issues error messagess, leaves the sysplex group, and deletes all DVIPA interfaces when a sysplex problem is detected. **X'0400', NMTP_GBCFSysMonNoJoin:** If set, the TCP/IP stack does not join the sysplex group until the V TCPIP,,SYSPLEX,JOINGROUP command is issued.
8(X'8')	NMTP_GBCFIqdVlanId	2	Binary	VLAN ID for the dynamic XCF HiperSockets interface. If not specified the value is 0.
10(X'A')	NMTP_GBCFSysWlmPoll	1	Binary	The number of seconds used by the sysplex distributor and its target servers, when polling WLM for new weight values.
11(X'B')	NMTP_GBCFZiipOptions	1	Binary	Workloads whose CPU cycles should be displaced to a zIIP. This field is valid only if the NMTP_GBCFZiip flag is set. The following are valid values: **X'80', NMTP_GBCFZiipIPSecurity:** If set, CPU cycles for IPSec workloads are displaced to a zIIP, when possible. **X'40', NMTP_GBCFZiipIqdioMultiWrite:** If set, CPU cycles for large TCP outbound messages are displaced to a zIIP.
12(X'C')	NMTP_GBCFSysMonTimerSecs	2	Binary	The number of seconds used by the sysplex monitor function to react to problems with needed sysplex resources.
14(X'E')	NMTP_GBCFXcfGroupId	2	EBCDIC	The 2-digit suffix used to generate the sysplex group name that the TCP/IP stack joins. If not specified the value is zero.
16(X'10')	NMTP_GBCFExpBindPortRangeBegNum	2	Binary	If flag NMTP_GBCFExpBindPortRange is set, this field contains the beginning port number in the reserved range.

Table 10. TCP/IP profile record Global configuration section (continued)

Offset	Name	Length	Format	Description
18(X'12')	NMTP_GBCFExpBindPortRangeEndNum	2	Binary	If flag NMTP_GBCFExpBindPortRange is set, this field contains the ending port number in the reserved range.
20(X'14')	NMTP_GBCFMaxRecs	4	Binary	Configured maximum records value for the D TCPIP,,NETSTAT command. The value range is 1 - 65535. The value 65536 indicates that the * (asterisk) value was specified. This means all records.
24(X'18')	NMTP_GBCFEcsaLimit	4	Binary	The maximum ECSA storage size in bytes that can be used by the TCP/IP stack.
28(X'1C')	NMTP_GBCFPoolLimit	4	Binary	The maximum private storage size in bytes that can be used in the TCP/IP address space.
32(X'20')	NMTP_GBCFWPQCV0Pri	1	Binary	The OSA-Express QDIO priority value that is assigned to packets represented by control value 0. This field is valid only if flag NMTP_GBCFWlmPriorityQ is set.
33(X'21')	NMTP_GBCFWPQCV1Pri	1	Binary	The OSA-Express QDIO priority value that is assigned to packets represented by control value 1. This field is valid only if flag NMTP_GBCFWlmPriorityQ is set.
34(X'22')	NMTP_GBCFWPQCV2Pri	1	Binary	The OSA-Express QDIO priority value that is assigned to packets represented by control value 2. This field is valid only if flag NMTP_GBCFWlmPriorityQ is set.
35(X'23')	NMTP_GBCFWPQCV3Pri	1	Binary	The OSA-Express QDIO priority value that is assigned to packets represented by control value 3. This field is valid only if flag NMTP_GBCFWlmPriorityQ is set.
36(X'24')	NMTP_GBCFWPQCV4Pri	1	Binary	The OSA-Express QDIO priority value that is assigned to packets represented by control value 4. This field is valid only if flag NMTP_GBCFWlmPriorityQ is set.
37(X'25')	NMTP_GBCFWPQCV5Pri	1	Binary	The OSA-Express QDIO priority value that is assigned to packets represented by control value 5. This field is valid only if flag NMTP_GBCFWlmPriorityQ is set.
38(X'26')	NMTP_GBCFWPQCV6Pri	1	Binary	The OSA-Express QDIO priority value that is assigned to packets represented by control value 6. This field is valid only if flag NMTP_GBCFWlmPriorityQ is set.
39(X'27')	NMTP_GBCFWPQFwdPri	1	Binary	The OSA-Express QDIO priority value that is assigned to forwarded packets. This field is valid only if flag NMTP_GBCFWlmPriorityQ is set.
40(X'28')	NMTP_GBCFAutoIQDX	1	Binary	AutoIQDX settings. If no flag bits are set, the NOAUTOIQDX parameter value is in effect. **X'02', NMTP_GBCFAutoIQDX_NoLargeData:** If this flag bit is set, dynamic IQDX interfaces are used for all eligible traffic, except for TCP data traffic that is sent with socket transmissions of 32 K or larger. **X'01', NMTP_GBCFAutoIQDX_AllTraffic:** If this flag bit is set, dynamic IQDX interfaces are used for all eligible traffic to the intraensemble data network.
41(X'29')	NMTP_GBCFPFidCnt	1	Binary	SMCR PFID count - the current number of configured PFID, port, and MTU entries in the NMTP_GBCFPFs array.

Table 10. TCP/IP profile record Global configuration section (continued)

Offset	Name	Length	Format	Description
42(X'2A')	NMTP_GBCFSMCGFlags	1	Binary	SMCGlobal flags: **x'80', NMTP_GBCFAUTOCACHE** AUTOCACHE is configured. This function is active only when flag NMTP_GBCFSMCR is set and field NMTP_GBCFPFidCnt is not zero, or flag NMTP_GBCFSMCD is set. **x'40', NMTP_GBCFAUTOSMC** AUTOSMC is configured.
43(x'2B')	NMTP_GBCFAdjDVMSS	1	Binary	ADJUSTDVIPAMSS settings. **x'80', NMTP_GBCFAdjDVMSS_AUTO** If this flag is set, TCP/IP automatically adjusts the MSS size to avoid fragmentation for TCP connections that use VIPAROUTE and distributed DVIPAs. **x'40', NMTP_GBCFAdjDVMSS_ALL** If this flag is set, TCP/IP automatically adjusts the MSS size to avoid fragmentation for TCP connections that use any DVIPA, distributed or not, as the source IP address. **x'20', NMTP_GBCFAdjDVMSS_NONE** If this flag is set, TCP/IP does not adjust the MSS for any TCP connections.
44(X'2C')	NMTP_GBCFFixedMemory	4	Binary	SMCR FIXEDMEMORY value in megabytes
48(X'30')	NMTP_GBCFTcpKeepMinInt	4	Binary	SMCR TCPKEEPMININTERVAL value in seconds
52(X'34')	NMTP_GBCFPFs(16)	96	Binary	SMCR PFID array that contains up to 16 entries. Each entry contains the following information: • PFID (2-byte hexadecimal value) • PortNum • MTU value
148(X'94')	NMTP_GBCFResv1	4	Binary	Reserved
152(X'98')	NMTP_GBCFFixedMemoryD	4	Binary	SMCD FIXEDMEMORY value in megabytes
156(X'9C')	NMTP_GBCFTcpKeepMinIntD	4	Binary	SMCD TCPKEEPMININTERVAL value in seconds
160(X'A0')		4	Binary	Reserved

TCP/IP profile record interface section

This section provides network interface information from the DEVICE, LINK, HOME, BSDROUTINGPARMS, and INTERFACE profile statements. For IPv4 interfaces, the IP address is included in the interface information. Only the subnet mask value from the BSDROUTINGPARMS statement is included in the interface information. For IPv6 interfaces, the IP addresses are provided in the IPv6 address section.

There can be multiple sections in the record, one per interface. Information from DEVICE, LINK, HOME, and BSDROUTINGPARMS statements for an interface is combined into one section. If more than one additional IPv4 loopback IP address has been configured, there are multiple sections for the IPv4 loopback interface, one per additional IP address.

Information for only the following types of network interfaces is provided in this section:

Loopback
The loopback section is provided only if additional loopback IP addresses besides the default address, 127.0.0.1, have been configured.

OSA-Express QDIO Ethernet
MPCIPA/IPAQENET or IPAQENET6

HiperSockets
MPCIPA/IPAQIDIO or IPAQIDIO6

Static MPC Point-to-point
MPCPTP or MPCPTP6

Static VIPA
VIRTUAL or VIRTUAL6

Information for dynamic XCF and dynamic VIPA interfaces is not supported in this section. Information for dynamic XCF interfaces can be found in the IPv4 and IPv6 configuration sections. Information for dynamic VIPA interfaces can be found in the dynamic VIPA address section.

If other types of network interfaces are defined to the TCP/IP stack, their presence is indicated by a flag bit in the NMTP_PICODepStmts and NMTP_PICODepChanged fields of the profile information common section.

Table 11 shows the TCP/IP profile record interface section.

Table 11. TCP/IP profile record interface section

Offset	Name	Length	Format	Description
0(X'0')	NMTP_INTFEye	4	EBCDIC	INTF eyecatcher

Table 11. TCP/IP profile record interface section (continued)

Offset	Name	Length	Format	Description
4(X'4')	NMTP_INTFFlags	4	Binary	Flags: **X'80000000', NMTP_INTFIPv6:** IPv6 indicator. If set, this entry is an IPv6 interface, otherwise this entry is an IPv4 interface. **X'40000000', NMTP_INTFDefIntf:** If set, the interface was defined by the INTERFACE statement; otherwise, the interface was defined by DEVICE and LINK statements. **X'20000000', NMTP_INTFIntfIDFlg:** If set, an IPv6 interface ID was specified. Field NMTP_INTFIntfID contains the interface ID value. **X'10000000', NMTP_INTFAutoRestart:** This flag applies only to non-VIRTUAL interfaces defined by DEVICE and LINK profile statements. If set, either AUTORESTART was specified or, the interface is using the same OSA-Express port, MPCPTP TRLE, or HiperSockets CHPID as an IPv6 interface, so the AUTORESTART parameter has been set by default. **X'08000000', NMTP_INTFIpBcast:** If set, IPBCAST was specified. **X'04000000', NMTP_INTFVlanIDFlg:** If set, VLANID was specified. Field NMTP_INTFVlanID contains the VLAN ID value. **X'02000000', NMTP_INTFMonSysplex:** If set, MONSYSPLEX was specified. **X'01000000', NMTP_INTFDynVlanReg:** If set, DYNVLANREG was specified. **X'00800000', NMTP_INTFVmac:** If set, VMAC was specified. Field NMTP_VmacAddr contains the virtual MAC address. **X'00400000', NMTP_INTFVmacAddrFlg:** If set, the VMAC parameter was specified with a virtual MAC address. If not set, the VMAC parameter was specified without a virtual MAC address. The OSA-Express QDIO feature generates the virtual MAC address. Field NMTP_VmacAddr contains the virtual MAC address.

Table 11. TCP/IP profile record interface section (continued)

Offset	Name	Length	Format	Description
4(X'4') (Cont)				**X'00200000', NMTP_INTFVmacRtLcl:** If set, VMAC was specified with the ROUTELCL subparameter. If not set, and flag NMTP_INTFVmac is set, then the ROUTEALL subparameter is in effect. **X'00100000', NMTP_INTFCheckSum:** If set, inbound checksum calculation is being performed. This flag applies only to MPCPTP interfaces. **X'00080000', NMTP_INTFSrcVipaIfNameFlg:** If set, SOURCEVIPAINTERFACE was specified. Field NMTP_INTFSrcVipaIntfName contains the specified source VIPA interface name. **X'00040000', NMTP_INTFTempPrefix:** If set, TEMPPREFIX was specified. Field NMTP_INTFTempPfxType indicates the type of IPv6 temporary address which was requested. **X'00020000', NMTP_INTFIsolate:** If set, ISOLATE was specified. This flag applies only to IPAQENET interfaces defined by the INTERFACE profile statement and to IPAQENET6 interfaces. **X'00010000', NMTP_INTFOptLatMode:** Indicates whether optimized latency mode (OLM parameter) was requested or is in effect. If set, and the interface is not active, the OLM parameter was specified for the interface. If set, and the interface is active, then the OLM setting is in effect for the interface. This flag applies to only IPAQENET interfaces defined by the INTERFACE profile statement and to IPAQENET6 interfaces. **X'00008000', NMTP_INTFChpIDFlg:** If set, an optional CHPID value was specified for an interface that was defined by the INTERFACE statement. The CHPID value is in NMTP_INTFChpID field. **X'00004000', NMTP_INTFTempIP:** If set, the TEMPIP value was specified for an interface that was defined by the INTERFACE statement. The NMTP_INTFIPv4Addr field is set to zeroes when this flag is set.

Table 11. TCP/IP profile record interface section (continued)

Offset	Name	Length	Format	Description
4(X'4') (Cont)				**X'00002000', NMTP_INTFSMCR:** If set, SMCR was specified or is in effect by default. This flag applies only to IPAQENET interfaces that the INTERFACE profile statement defines and to IPAQENET6 interfaces. **X'00001000', NMTP_INTFSMCD:** If set, SMCD was specified or is in effect by default. This flag only applies to: • IPAQENET and IPAQIDIO interfaces that the INTERFACE profile statement defines • IPAQENET6 and IPAQIDIO6 interfaces
8(X'8')	NMTP_INTFType	1	Binary	Type of interface: **NMTP_INTFTLOOPB(1):** Loopback (LOOPBACK/LOOPBACK6) **NMTP_INTFTOSAETH(2):** OSA-Express QDIO Ethernet (IPAQENET/IPAQENET6) **NMTP_INTFTHIPERSOCK(3):** HiperSockets (IPAQIDIO/IPAQIDIO6) **NMTP_INTFTPTP(4):** MPC Point-to-point (MPCPTP/ MPCPTP6) **NMTP_INTFTVIRTUAL(5):** Static Virtual (VIRTUAL/VIRTUAL6)
9(X'9')	NMTP_INTFRtrType	1	Binary	Router type. This field is valid only when the NMTP_INTFType field value is NMTP_INTFTOSAETH. **NMTP_INTFRTNON(1):** NONROUTER **NMTP_INTFRTPRI(2):** PRIROUTER **NMTP_INTFRTSEC(3):** SECROUTER

Table 11. TCP/IP profile record interface section (continued)

Offset	Name	Length	Format	Description
10(X'A')	NMTP_INTFReadStorType	1	Binary	Read storage amount type. This field is valid only when the NMTP_INTFType field value is NMTP_INTFTOSAETH or NMTP_INTFTHIPERSOCK. **NMTP_INTFRSGLOBAL(1):** GLOBAL **NMTP_INTFRSMAX(2):** MAX **NMTP_INTFRSAVG(3):** AVG **NMTP_INTFRSMIN(4):** MIN
11(X'B')	NMTP_INTFInbPerfType	1	Binary	Inbound performance type. This field is valid only when the NMTP_INTFType field value is NMTP_INTFTOSAETH. **NMTP_INTFIPBAL(1):** BALANCED **NMTP_INTFIPDYN(2):** DYNAMIC **NMTP_INTFIPMINCPU(3):** MINCPU **NMTP_INTFIPMINLAT(4):** MINLATENCY
12(X'C')	NMTP_INTFSecClass	1	Binary	SECCLASS value.
13(X'D')	NMTP_INTFChpID	1	Binary	CHPID value. This field is valid only for the following interface types: • IPv6 interfaces or IPv4 interfaces that are defined by the INTERFACE statement where the NMTP_INTFType field value is NMTP_INTFTHIPERSOCK. • Interfaces for which the NMTP_INTFChpIDFlg flag is set.
14(X'E')	NMTP_INTFDupAddrDet	1	Binary	DUPADDRDET count. This field is valid only for IPv6 interfaces, where the NMTP_INTFType field value is NMTP_INTFTOSAETH.
15(X'F')	NMTP_INTFIPv4Mask	1	Binary	IPv4 Subnet number of mask bits from INTERFACE or BSDROUTINGPARMS statement. If subnet mask specified on BSDROUTINGPARMS but overridden by OMPROUTE, this field is zero.

Table 11. TCP/IP profile record interface section (continued)

Offset	Name	Length	Format	Description
16(X'10')	NMTP_INTFTempPfxType	1	Binary	TEMPPREFIX type. This field is valid only for IPv6 interfaces where flag NMTP_INTFTempPfx is set, and the NMTP_INTFType field value is NMTP_INTFTOSAETH. **NMTP_INTFTTALL(1):** ALL **NMTP_INTFTTPFX(2):** Prefix specified **NMTP_INTFTTNONE(3):** NONE **NMTP_INTFTTDIS(4):** Temporary IPv6 address generation is disabled due to multiple Duplicate Address Detection (DAD) failures.
17(X'11')	NMTP_INTFDynTypes	1	Binary	Indicates the dynamic inbound performance types. This field is set only when the NMTP_INTFInbPerfType field is set to NMTP_INTFIPDYN and the interface was defined by an INTERFACE statement. • X'80', NMTP_INTFDYNWRKLDQ: If set, INBPERF DYNAMIC WORKLOADQ was configured.
18(X'12')	NMTP_INTFChpIDType	1	Binary	The CHPID type of the OSA-Express QDIO Ethernet interface. This field is valid only for interfaces where the NMTP_INTFType field value is NMTP_INTFTOSAETH and the interface was defined by an INTERFACE profile statement (flag NMTP_INTFDefIntf is set). **NMTP_INTFCTOSD(1):** OSD indicates an external data network CHPID type **NMTP_INTFCTOSX(2):** OSX indicates an intraensemble data network CHPID type
19(X'13')		1	Binary	Reserved
20(X'14')	NMTP_INTFVlanID	2	Binary	VLAN ID. This field is valid only when flag NMTP_INTFVlanIDFlg is set and the NMTP_INTFType field value is NMTP_INTFTOSAETH or NMTP_INTFTHIPERSOCK.
22(X'16')	NMTP_INTFMtu	2	Binary	MTU value. This field is valid only when flag NMTP_INTFDefIntf is set, and the NMTP_INTFType field value is NMTP_INTFTOSAETH or NMTP_INTFTHIPERSOCK.
24(X'18')	NMTP_INTFIPv4Addr	4	Binary	If flag NMTP_INTFIPv6 is not set, this field is the IPv4 IP address from the HOME or INTERFACE statement. If an IP address has not been configured for the interface or if the NMTP_INTFTempIP field is set, this field is set to zeros.

Table 11. TCP/IP profile record interface section (continued)

Offset	Name	Length	Format	Description
28(X'1C')	NMTP_INTFIfIndex	4	Binary	The interface index, which is a small, positive number assigned to the interface when it is defined to the TCP/IP stack. For interfaces defined by DEVICE and LINK statements, this is the interface index of the LINK.
32(X'20')	NMTP_INTFVmacAddr	6	Binary	Virtual MAC address. This field is valid only if flag NMTP_INTFVmac is set. The field contains one of the following values: • If flag NMTP_INTFVmacAddrFlg is set, the field contains the configured virtual MAC address. • If flag NMTP_INTFVmacAddrFlg is not set, and the interface is active, the field contains the virtual MAC address generated by the OSA-Express QDIO feature, when the interface was activated. If the interface is not yet active, then the field is set to zeros.
38(X'26')		2	Binary	Reserved
40(X'28')	NMTP_INTFIntfID	8	Binary	IPv6 interface ID value. This field is valid only if flag NMTP_INTFIntfIDFlg is set.
48(X'30')	NMTP_INTFName	16	EBCDIC	Interface name. For interfaces defined by DEVICE and LINK statements, this is the LINK name; otherwise, it is the interface name defined on the INTERFACE statement.
64(X'40')	NMTP_INTFAssocName	16	EBCDIC	One of the following associated names: • DEVICE name for interfaces defined with the LINK profile statement. For IPAQENET interfaces defined with the LINK statement, this is also the OSA-Express port name. For MPCPTP interfaces defined with the LINK statement, this is also the TRLE name. • PORTNAME value from the IPAQENET/IPAQENET6 INTERFACE statement. • TRLENAME value from the MPCPTP6 profile statement.
80(X'50')	NMTP_INTFSrcVipaIntfName	16	EBCDIC	Source VIPA interface name from the INTERFACE profile statement. This field is valid only if flag NMTP_INTFSrcVipaIfNameFlg is set.

Chapter 5. IP Diagnosis Guide

OPTIONS keywords

The following keywords are used for the OPTIONS component routine parameters. You can enter complete keywords. You can also enter a portion of the characters to make the keyword distinguishable from other keywords. For example, for the DISCARD keyword, you can enter DISCARD, DISCAR, DISCA, DISC, DIS, or DI.

AH Select packets with an AH extension header.

ASCII
Packet trace data dumped is shown in hexadecimal and interpreted in ASCII translation only. The default is BOTH.

BASIC ([DETAIL|SUMMARY])
For specific packet types, format each element of the packet data. This parameter applies to DNS, RIP, and SNMP packet data.

DETAIL
Format the IP header, protocol header, and protocol data in as few lines as possible. DETAIL is the default.

SUMMARY
Format the IP and protocol headers in as few lines as possible.

BOOTP[(port_number|67 port_number|68)]
Select BOOTP and DHCP protocol packets. The port_number defines the BOOTP and DHCP port numbers to select packets for formatting. Equivalent to PORT(67 68).

BOTH
Packet trace data dumped is shown in hexadecimal and interpreted with both ASCII and EBCDIC translations. The default is BOTH.

BROADCAST
Select packets with a broadcast IPv4 address. Equivalent to IPADDR(255.255.255.255/255.255.255.255).

CHECKSUM [(DETAIL|SUMMARY)]
The selected packets have their checksum values validated.

DETAIL
If there is a checksum error, then the packet is formatted and dumped.

SUMMARY
A message is issued for each packet that encounters a checksum error. SUMMARY is the default.

CID
Select data trace records that contain the specific connection ID value. The connection ID value can be determined from the Netstat COnn/-c report. For TCP connections across Shared Memory Communications, data trace records can be selected by using the local SMC link ID (LocalSMCLinkId). This SMC link ID can be determined from the Netstat ALL/-A or Netstat DEvlinks/-d report. Up to 16 values or ranges can be specified.

CLASSA
Select packets with a class A IPv4 address. Equivalent to IPADDR(0.0.0.0/128.0.0.0).

CLASSB
Select packets with a class B IPv4 address. Equivalent to IPADDR(128.0.0.0/192.0.0.0).

CLASSC
Select packets with a class C IPv4 address. Equivalent to IPADDR(192.0.0.0/224.0.0.0).

CLASSD
Select packets with a class D IPv4 address. Equivalent to IPADDR(224.0.0.0/240.0.0.0).

CLASSE
Select packets with a class E IPv4 address. Equivalent to IPADDR(240.0.0.0/248.0.0.0).

CLEANUP(nnnnn|500)
Defines a record interval where saved packet information in storage is released. The minimum value is 500 records; the maximum value is 1048576 records; the default is 500 records. If you set the record interval to 0, cleanup does not occur.

DATASIZE (data_size|0)
Selects packets that contain more protocol data than the data_size value. The minimum value is 0. The maximum value is 65535. The data size is determined from the amount of packet data available minus the size of any protocol headers. Equivalent to FLAGS(DATA).

DATTRACE
Select packets that are written from the VARY TCPIP,,DATTRACE command.

DEBUG(debug_level_list)
Provides documentation about SYSTCPDA format processing. debug_level_list is a list of numbers from 1 to 64. Use only under the direction of an IBM Service representative.

DELAYACK(threshold|200)
The delay acknowledgment threshold in milliseconds used in the calculation of round-trip time in the TCP session report. The minimum value is 10 milliseconds. The maximum value is 1000 milliseconds. The default value is 200 milliseconds.

DEVICEID(device_id)
Selects packets that are written to or received from an OSAENTA trace with one of the specified device identifiers. One to 16 device IDs can be specified. This filter applies only to type 7 trace records. The device_id value is a hexadecimal number in the form X'*csmfclua*':

cs The channel subsystem ID for this datapath device.

mf The LPAR Multiple Image Facility ID for the LPAR that is using this datapath device.

cl The control unit logical identifier for this datapath device.

ua The unit address for this datapath device.

Each identifier is a two-digit hexadecimal value in the range 00 - FF.

Tip: You can obtain the *device_id* values for any active user of the OSA by using the Hardware Management Console (HMC). For a data device that is active on a z/OS stack, you can obtain the *device_id* value for that data device from message IST2190I of the output from the D NET,TRLE command.

DEVTYPE(device_type_list)
Select packets that are written to or received from an interface with one of the specified device types. From 1 to 16 types can be specified. This does not apply to data trace records. The following types can be specified:

- ATM
- CDLC
- CLAW
- CTC
- ETHER8023
- ETHERNET
- ETHEROR8023
- FDDI
- HCH
- IBMTR
- IPAQENET
- IPAQENET6
- IPAQIDIO
- IPAQIDIO6
- IPAQTR
- IQDX
- IQDX6
- LOOPBACK
- LOOPBACK6
- MPCPTP
- MPCPTP6
- OSAFDDI
- OSAENET
- SNALINK
- SNALU62
- VIRTUAL
- VIRTUAL6
- X25NPSI

DISCARD(reason_code_list)
Select packets with one of the specified discard reason codes. Up to 16 discard reason codes can be specified in the range 0 - 65535. Each entry in the list can be a range: low_number:high_number. Values can be decimal or hexadecimal.

```
    0
      Packet was not discarded
    1:4087     A packet was discarded by OSA-Express
    1:1023     Select packets discarded by OSA-Express for DISCARD=EXCEPTION
reasons
    4096:8191  IP packet was discarded by TCPIP
    8192:12287 TCP packet was discarded by TCPIP
```

See z/OS Communications Server: IP and SNA Codes for the TCP/IP discard reason codes.

DNS[(port_number|53)]
Select Domain Namer Service protocol packets. The port_number defines the DNS port number to select packets for formatting. Equivalent to PORT(53).

DOMAIN[(port_number|53)]
Select Domain Namer Service protocol packets. The port_number defines the DNS port number to select packets for formatting. Equivalent to PORT(53).

DUMP[(nnnnn|65535)]
Dump the selected packets in hexadecimal with EBCDIC and ASCII translations. The IP and protocol headers are dumped separately from the packet data. The value *nnnnn* represents the maximum amount of packet data that is to be dumped from each packet. The default value is 65535 bytes. The minimum value is 0. The maximum value is 65535. The IP and protocol headers are not subject to this maximum.

The default report options are DUMP and FORMAT.

The BOTH, ASCII, EBCDIC, and HEX keywords describe how the dumped packets are translated. The default is BOTH. The display can be changed by using these keywords. The default ASCII translation table is used. This table might not match the table that is being used by the application. When you are formatting the CTRACE, it is helpful to have the correct line length. Use the IPCS PROFILE LINESIZE command to set the line length. For example,

```
IPCS PROFILE LINESIZE(80)
```

sets the maximum line length to 80 characters so that all formatted data is viewable within 80 characters.

If the STREAM report is chosen, then the dump of the packets is deferred until the stream of data is collected.

EBCDIC
Packet trace data dumped is shown in hexadecimal and interpreted with EBCDIC translation only. The default is BOTH.

EE Select Enterprise Extender (EE) protocol packets. The port number defines the first EE port number to select packets for formatting. The EE port number and the next four port numbers are used. Equivalent to PORT(12000:12004).

ELEMENT(element_number_list)
Select SNA protocol packets with a matching origin or destination element address in the TH2 or TH4 transmission header. Valid values are in the range 0 - 65535. Up to 16 element numbers can be specified.

ESP
Select packets with a protocol number of 50. Equivalent to PROTOCOL(50).

ETHTYPE(*type*)
Selects packets that are written to or received from an OSAENTA trace with one of the specified frame types. From 1 to 16 types can be specified. This filter applies only to type 7 trace records. The following types can be specified:

```
x'0800'  for IP
x'86DD' for IPV6
x'0806' for ARP
x'80d5' for SNA
```

EXPORT[(DETAIL|SUMMARY)]
The selected packets are written to the EXPORT data set in .CSV (Comma Separated Value) format. In .CSV format, each character field is surrounded by double quotation marks and successive fields are separated by commas. The first line of the file defines the fields. Each subsequent line is a record that contains the values for each field.

DETAIL
Format the IP header, protocol header, and protocol data as separate lines of data.

SUMMARY
Format the IP header and protocol header in one line of data. SUMMARY is the default.

Allocate a file with DDNAME of EXPORT before you invoke the CTRACE command with EXPORT in the OPTIONS string.

```
ALLOC
FILE(EXPORT) DA(PACKET.CSV) SPACE(15 15) TRACK
```

The record format is variable block with logical record length of 512 bytes.

FINGER[(port_number|79)]
Select FINGER protocol packets. The port_number defines the FINGER port number to select packets for formatting. Equivalent to PORT(79).

FIRST|LAST
Selects which packet in a set of encapsulated packets is used for selection. An example is the ICMP error report packet that contains the IP header that is in error. FIRST indicates that the ICMP packet is used for selection. LAST indicates that the last encapsulated IP header is used for selection. FIRST is the default.

If a packet is encapsulated for IPSec with Encapsulating Security Payload (ESP), all inner packets are encrypted. In this case, FIRST is used for selection when these packets are analyzed.

FLAGS(flags list)
Select packets that have the matching characteristics. Flags that can be specified are:

ALL When more than one flag is specified, the packet must meet all the criteria of the flags requested. ALL is the default.

ANY When more than one flag is specified, the packet need meet only one of the criteria of the flags requested.

ABBREV
Select packets that are abbreviated.

ACK Select packets that have a TCP header with the ACK flag set.

BAD Select packets that might be too short to contain all the required headers

BBI The SNA packet contains a begin bracket indicator.

BCI The SNA packet contains a begin chain indicator.

CDI The SNA packet contains a change direction indicator.

CEBI The SNA packet contains a conditional end bracket indicator.

CKSUM
Select packets that have a check sum error

CLC The SMC Connection Layer Control packets

CSI The SNA packet contains a code selection indicator.

DATA Selects packets that contain data.

DF Select packets that have a non-zero discard code. These packets are discarded by TCP/IP.

DFC The SNA packet is a data flow control packet.

DISCARD
Select packets that have a non-zero discard code. These packets are discarded by OSA-Express or by TCP/IP.

DR1 The SNA packet is requesting a DR1 response.

DR2 The SNA packet is requesting a DR2 response.

EBI The SNA packet contains an end bracket indicator.

ECI The SNA packet contains an end chain indicator.

EDI The SNA packet contains an enciphered data indicator.

ERI The SNA packet is an error response.

FI The SNA packet contains formatted data.

FIB The SNA packet is the first packet of a bracket (or of a conditional begin bracket). The RH BBI flag is set and the EBI flag is not.

FIC Select packets that are the first in chain SNA RU.

FIN Select packets that have a TCP header with the FIN flag set.

FIS Select packets that are in the first fragment of an IPv4 or IPv6 packet or the first segment of a SNA PDU.

FMD The SNA packet is a function management data packet.

FMH The SNA packet is a function management data header.

FRAME
Selects OSAENTA packets that have a frame header.

FULL Select packets that are complete.

HOME
Select packets that have an IP destination address equal to the IP source address.

IN Select packets that are inbound.

IPEXT Select packets that have an extension header.

IPO Select packets that have an IPv4 header options field.

IPV4 Select IPv4 packets. IPv4 cannot be used in combination with other data selectors that are IPv6-specific, such as LINKLOCAL.

IPV6 Select IPv6 packets. IPv6 cannot be used in combination with other data selectors that are IPv4-specific, such as BROADCAST.

IPV6EXT
Select packets that have an extension header. IPV6EXT is equivalent to IPEXT.

IQDXND
Select ICMPV6 Neighbor Advertisement and Neighbor Solicit packets on an IQDX device.

LIB The SNA packet is a last packet of a bracket. The RH BBI flag is not set and the EBI flag is set.

LIC Select packets that are the last in a chain of SNA RUs.

LIS Select packets that are the last fragment of an IPv4 or IPv6 packet or the last segment of a SNA PDU.

LPAR Select NTA packets that are transmitted between LPARs shared by an OSA-Express device.

L2 The OSAENTA packet is from a layer 2 OSA application.

L3 The OSAENTA packet is from a layer 3 OSA application (like TCP/IP).

MIB The SNA packet is in the middle of a bracket. The RH BBI flag is not set and the EBI flag is not set.

MIC Select packets that are the middle fragment of an IPv4 or IPv6 packet.

MIS Select packets that are the middle fragment of an IPv4 or IPv6 packet or the middle segment of a SNA PDU.

NC The SNA packet is a Network Control packet.

NTA Select OSAENTA packets.

OFFLOAD
Select outbound packets for which segmentation is offloaded.

OIB The SNA packet is the only packet of a bracket. The RH BBI flag is set and the EBI flag is set.

OIC Select packets that are only in a chain SNA RH request.

OIS Select packets that are IPv4 or IPv6 packets that are not fragmented or that are the only segment of a SNA PDU.

OUT Select packets that are outbound.

PDI Select SNA packets with the padded data indicator.

PDU The IP packets that are packed by TCP/IP into a single PDU buffer.

PI The SNA packet contains a pacing indicator.

PING Select packets that are ICMP/ICMPv6 echo request and echo reply.

PSH Select packets that have a TCP header with the PSH flag set.

QID Select packets that have a QID value greater than one.

QRI The SNA packets with a queued response indicator

REQ The SNA packet is a request.

RESP The SNA packet is a response.

RLWS Select SNA packets with the request large window size indicator.

RSM Select packets that are reassembled.

RST Select packets that have a TCP header with the RST flag set.

SC The SNA packet is a session-control packet.

SDI The SNA packet contains sense data.

SEG Select packets that are segmented.

SMC Select SMC packets.

SNA Select SNA packets.

SYN Select packets that have a TCP header with the SYN flag set.

TCPO Select packets that have a TCP header options field.

TOS Select IPv4 packets that have a nonzero value in the ip_tos field.

TUNNEL
Select packets with protocol number 47 GRE or 41 (IPv6 over IPv4). z/OS Communications Server currently does not support IPv6 over IPv4 (protocol number 41).

URG Select packets that have a TCP header with the URG flag set.

VLAN Select packets that have a VLAN 802.1q tag

ZWIN Select packets that have a TCP header with a zero window value.

Notes:

- The use of the FIC, MIC, and LIC flags require the use of the NOREASSEMBLY option.
- When a packet is reassembled, then it becomes an OIC packet with the RSM flag set.
- Do not intermix SNA and IP flags.

Table 12. Flags that apply to IP or SNA packets

Flag	Applies to IP	Applies to SNA	Comments
ABBREV	Y	Y	
BAD	Y	Y	
BBI	N	Y	
BCI	N	Y	
CDI	N	Y	
CEBI	N	Y	
CI	N	Y	
CKSUM	Y	N	
CLC	Y	N	
CSI	N	Y	
DATA	Y	Y	
DF	Y	N	
DFC	N	Y	
DISCARD	Y	Y	
DR1	N	Y	
DR2	N	Y	
EBI	N	Y	
ECI	N	Y	
EDI	N	Y	
ERI	N	Y	
FI	N	Y	
FIB	N	Y	
FIC	N	Y	
FIN	Y	N	TCP only
FIS	Y	Y	

Table 12. Flags that apply to IP or SNA packets (continued)

Flag	Applies to IP	Applies to SNA	Comments
FM	N	Y	
FMD	N	Y	
FMH	N	Y	
FRAME	N	Y	OSAENTA only
FULL	Y	Y	
HOME	Y	N	
IN	Y	Y	
IPEXT	Y	N	
IPO	Y	N	
IPV4	Y	N	
IPV6	Y	N	
IPV6EXT	Y	N	
LIB	N	Y	
LIC	N	Y	
LIS	Y	Y	
LPAR	Y	Y	OSAENTA only
L2	Y	Y	OSAENTA only
L3	Y	Y	OSAENTA only
MIB	N	Y	
MIC	N	Y	
MIS	Y	Y	
NC	N	Y	
NTA	Y	Y	OSAENTA only
OFFLOAD	Y	N	TCP only
OIB	N	Y	
OIC	N	Y	
OIS	Y	Y	
OUT	Y	Y	
PDI	N	Y	
PDU	Y	N	SYSTCPDA only
PI	N	Y	
PING	Y	N	
PSH	Y	N	TCP only
QID	Y	Y	OSA-Express 3 or later ports with QDIO inbound workload queueing enabled.
QRI	N	Y	
REQ	N	Y	
RESP	N	Y	

Table 12. Flags that apply to IP or SNA packets (continued)

Flag	Applies to IP	Applies to SNA	Comments
RLWS	N	Y	
RSM	Y	N	
RST	Y	N	TCP only
SC	N	Y	
SDI	N	Y	
SEG	Y	Y	
SMC	Y	N	
SYN	Y	N	TCP only
TCPO	Y	N	TCP only
TOS	Y	Y	SNA TPF field
TUNNEL	Y	Y	
URG	Y	N	TCP only
VLAN	Y	Y	OSAENTA only
ZWIN	Y	N	TCP only

FMT
Equivalent to FORMAT.

FORMAT[(DETAIL|SUMMARY ALL|FIRST|LAST)]
The selected packets with defined packet data are to be formatted. The SHORT keyword on the CTRACE command selects this option if no other report options are specified. The default report options are DUMP and FORMAT.

DETAIL
Format the IP header, protocol header, and the protocol data.

SUMMARY
Format the IP header and protocol header. DETAIL is the default.

ALL
Format all encapsulated packets. ALL is the default.

FIRST
Format the first encapsulated packet.

LAST
Format the last encapsulated packet

An example of an encapsulated packet is an ICMP error report.

FTP[(data_port_number|20 control_port_number|21)]
Select FTP protocol packets. The port_number defines the FTP port numbers to select packets for formatting. Equivalent to PORT(20,21).

FULL
Equivalent to DUMP and FORMAT. The FULL keyword on the CTRACE command selects this option if no other report options are specified.

GAIN(rtgain|125,vargain|250)
Values of the round-trip gain (rtgain) and the variance gain (vargain), in milliseconds, used in the calculation of round-trip time in the TCP session report. Valid values are in the range 0 - 1000. The default value for rtgain is 125. The default value for vargain is 250.

GOPHER[(port_number|70)]
Select GOPHER protocol packets. The port_number defines the GOPHER port numbers to select packets for formatting. Equivalent to PORT(70).

GRE
Select packets with a protocol number of 47. Equivalent to PROTOCOL(47).

GMT
Format the time stamps in GMT time. The default is the value that is specified on the CTRACE subcommand.

HEX
Packet trace data dumped is shown in hexadecimal only with no translation. The default is BOTH.

HPRDIAG[(SUMMARY)]
Select high-performance routing (HPR) packets and group them by transport connection identifier (TCID). The report shows session information that can be helpful for HPR diagnosis.

HOST
Select packets with a host IP address. Equivalent to IPADDR(0.0.0.0/255.255.0.0)

HTTP[(port_number|80)]
Select HTTP protocol packets. The port_number defines the HTTP port numbers to select packets for formatting. Equivalent to PORT(80). See "WWW[(port_number|80)]" on page 219.

ICMP
Select packets with a protocol number of 1. Equivalent to PROTOCOL(1).

ICMP6 or ICMPV6
Select packets with a protocol number of 58. Equivalent to PROTOCOL(58).

IGMP
Select packets with a protocol number of 2. Equivalent to PROTOCOL(2).

INTERFACE(interface_name_list) or LINKNAME(interface_name_list)
Select packet trace records with the specified interface name. Up to 16 interface names can be specified. Each interface name can be up to 16 characters. Use an asterisk (*) as a wildcard to replace characters at the end of the interface name.

IPADDR(ipaddr[/mask_or_prefixlength]|X'hhhhhhhh'[]-nnnnn[)
Select packets with a matching IP address, optional IPv4 address mask or IPv6 prefix length and optional port number. Up to 16 IP addresses can be specified. The IPADDR is specified in three parts:

1. An IPv4 or IPv6 address

   The IPv4 address can be in dotted decimal notation, a keyword, or a hex value.

   - IPv4 dotted decimal notation

     `127.0.0.1`

   - IPv4 keyword

     A A class A IPv4 address, 0.0.0.0/128.0.0.0

     B A class B IPv4 address, 128.0.0.0/192.0.0.0

     C A class C IPv4 address, 192.0.0.0/224.0.0.0

     D A class D IPv4 address, 224.0.0.0/240.0.0.0

     E A class E IPv4 address, 240.0.0.0/248.0.0.0

H A local host address, 0.0.0.0/0.0.255.255

L An IPv4 or IPv6 loopback address, 127.0.0.0/255.0.0.0 or ::1

M The broadcast IPv4 address, 255.255.255.255/255.255.255.255

***** Any address, 0.0.0.0/0.0.0.0

0 An IPv4 or IPv6 address of zero, 0.0.0.0/255.255.255.255 or ::/128

- IPv4 or IPv6 address as a hexadecimal number up to 32 (IPv4) or 128 (IPv6) digits

  `X'7f000001'`
- IPv6 address

  `1080::8:800:200C:417A`

2. An IPv4 address mask or IPv6 prefix length

   The IPv4 address mask (1 - 32) or IPv6 prefix length (1 - 128) is preceded by a slash(/). Specify an IPv4 address mask only when the IPv4 address is in dotted decimal notation. The IPv4 address mask can be in dotted decimal notation, for example: `9.37/255.0.0.0 or 9.37/255.255.0.0`
3. A port number

   The port number is preceded by a dash (-). It is a decimal number in the range 0 - 65535.

Notes:

- There should be no spaces between the IP addresses and the subnet masks.
- The BROADCAST, CLASSA, CLASSB, CLASSC, CLASSD, CLASSE, HOST, LINKLOCAL, LOOPBACK, MULTICAST, and SITELOCAL keywords add to the total of 16 IP addresses.
- The port number when used adds to the total of 16 port numbers in the PORT keyword.
- IPv4 addresses and IPv4 - mapped IPv6 addresses are treated as equivalent addresses.

IPID(ipid_number_list)
Select packets that match the ip_id number in the IPv4 packet header. Up to 16 ID numbers can be specified in the range 0 - 2147483647 or 0 - X'FFFFFFF'. Each entry in the list can be a range: low_number:high_number. Values can be decimal (nnnnn) or hexadecimal (X'hhhh'). If the packets are fragmented, specify NOREASSEMBLY to select each packet.

Tip: Associated encrypted text is not readable.

IPv4
Equivalent to FLAGS(IPV4).

IPv6
Equivalent to FLAGS(IPV6).

IKE
Select ISAKMP protocol packets. Equivalent to PORT(500). See the ISAKMP keyword.

ISAKMP
Select ISAKMP protocol packets. Equivalent to PORT(500). See the IKE keyword.

JOBLIST|JOBNAME(job_name_list)
Select data trace records with the specified JOBNAME. Up to 16 job names can

be specified. Each job name can be up to eight characters. If the last character of a job name is an asterisk (*), then only the characters up to the asterisk are compared.

The CTRACE JOBLIST/JOBNAME parameter provides the same function, except that wildcards are not supported.

LIMIT(record_count)

record_count
The maximum number of records that are formatted. The default value 999999999 records.

Guideline: This keyword is also accepted if specified on the CTRACE subcommand.

LINKLOCAL
Select packets with an IPv6 link-local unicast prefix. Equivalent to IPADDR(FE80::/10).

LINKNAME(link_name_list)
Select packet trace records with the specified LINKNAME. Up to 16 link names can be specified. Each link name can be up to 16 characters. If the last character of a link name is an asterisk (*), then only the characters up to the asterisk are compared.

The CTRACE JOBLIST/JOBNAME parameter provides the same function, except that wildcards are not supported and only the first eight characters of the link name are compared.

LOCAL
Format the time stamps in local time. The default is the value that is specified on the CTRACE subcommand.

LOOPBACK
Select packets with either an IPv4 or IPv6 loop back address. Equivalent to IPADDR(127.0.0.0/255.0.0.0::1). If other addresses are defined as loopback, they can be selected explicitly by using IPADDR().

LOOPBACK6
Select packets with an IPv6 loop back address. Equivalent to IPADDR(::1). If other addresses are defined as loopback, they can be selected explicitly by using IPADDR().

MACADDR(macaddr)
Selects packets that are written to or received from an OSAENTA trace with one of the specified MAC addresses. From 1 to 16 addresses can be specified. This filter applies only to type 7 trace records. A MACADDR is 12 hexadecimal digits.

MULTICAST
Select packets with either an IPv4 or IPv6 multicast address. Equivalent to CLASSD IPADDR(FF00::/8).

NAT
Select NAT protocol packets. Equivalent to PORT(4500).

NOCHECKSUM
The selected packets do not have their checksum values validated. CHECKSUM is the default.

NOREASSEMBLY
Do not reassemble fragmented IP packets into a complete packet. REASSEMBLY is the default.

NOSEGMENT
Packet trace records that span multiple CTRACE records are not recombined. Only the first segment record of packet is used. The rest of the segment records are discarded. SEGMENT is the default.

NOT
If the NOT option is selected then any selection criteria is reversed. If a record matches the selection criteria, it is not processed. If a record does not match the selection criteria, it is processed.

NTP[(port_number|123)]
Select NTP protocol packets. The port number defines the NTP port number to select packets for formatting. Equivalent to PORT(123).

OPTION
The selected options with defaults are listed.

OSPFI
Select packets with a protocol number of 89. Equivalent to PROTOCOL(89).

PACKETTRACE
Select packets that are written from the VARY TCPIP,,PKTTRACE command.

IPEXT
Select packets with an extension header.

PORT(port_number_list)
Select packets with one of the specified port numbers. Up to 16 port numbers can be specified in the range 0 - 65535. Each entry in the list can be a range: `low_number:high_number`. Values can be decimal (nnnnn) or hexadecimal (X'hhhh'). The following keywords add to the list of 16 port numbers:

- BOOTP
- DHCP
- DNS
- DOMAIN
- EE
- FINGER
- GOPHER
- HTTP
- NAT
- IKE
- RIP
- NTP
- ROUTER
- RPC
- SASP
- SMTP
- SNMP
- TELNET
- TFTP
- TIME

- WWW

PROTOCOL(protocol number list)
Select packets with one of the specified protocol numbers. Up to 16 protocol numbers can be specified in the range 0 - 255. Each entry in the list can be a range: `low_number:high_number`. Values can be decimal (nnn) or hexadecimal (X'hh').

Protocol filters on only the upper-layer header of an IPv6 packet. It does not filter for IPv6 extension headers (Hop-by-Hop Options, Routing, Fragment). Instead, IPv6 extension headers are included in the display of the basic IPv6 header. The following keywords add to the list of 16 protocol numbers:

- AH
- ESP
- GRE
- ICMP
- ICMP6,
- ICMPV6
- IGMP
- OSPFI
- TCP
- UDP

QOS(quality_of_service_list)
Select the records with the matching quality of service from the IPv4 Type of Service field. Up to 16 QoS values can be specified in the range 0 - 7. Each entry in the list can be a range: `low_number:high_number`. Values can be decimal (n) or hexadecimal (X'h').

QID(qid_list)
Select the records with the matching read queue identifier (QID) from the OSA-Express 3 or later ports with QDIO inbound workload queueing enabled. QID 1 selects records that are received on the primary input queue, and subsequent QIDs select records from the corresponding ancillary input queue (AIQ). Up to 16 QID values can be specified in the range 0 - 8. Each entry in the list can be a range: `low_number:high_number`. Values can be decimal (n) or hexadecimal (X'h').

REASSEMBLY[(packet_size|65535,DETAIL|SUMMARY)]
Reassemble IP fragments into a complete packet.

packet_size
The maximum size of a reassembled packet that is allowed. The smallest value that is allowed is 576 bytes, the largest is 65535 bytes. The default value is 65535 bytes.

DETAIL
List each of the reassembly statistics for each packet when a packet completes reassembly.

SUMMARY
Show only the reassembly statistics and information about packets that did not complete reassembly.

REASSEMBLY(65535,SUMMARY) is the default.

RECORDS(record_number_list)
Select the records with matching record numbers in the trace data. Up to 16

record numbers can be specified. Record numbers are assigned after any IPCS CTRACE selection criteria are met. Each entry in the list can be a range: `low_number:high_number`. Values can be decimal (nnnnnnnnnn) or hexadecimal (X'hhhhhhhh').

RIP[(port_number|520)]
Select RIP protocol packets. The port_number defines the RIP port number to select packets for formatting. Equivalent to PORT(520).

ROUTER[(port_number|520)]
Select RIP protocol packets. The port_number defines the RIP port number to select packets for formatting. Equivalent to PORT(520).

RIPNG
Select packets with a port number of PORT(521). Equivalent to PORT(521).

RPC[(port_number|111)]
Select RPC protocol packets. The port_number defines the RPC port number to select packets for formatting. Equivalent to PORT(111).

SASP (port_number|3860)
Select z/OS Load Balancing Advisor port numbers. The port_number defines the SASP port number to select packets for formatting. Equivalent to PORT(3860).

SEGMENT
Packet trace records that span multiple CTRACE records are recombined. Data from segment records is saved until all the CTRACE records are read to recreate the original packet. SEGMENT is the default.

SESSION[(DETAIL|PIPE|STATE|SUMMARY)]
Generate a report that shows TCP or UDP session traffic.

DETAIL
List each of the packets for a session, as well as the summary statistics. DETAIL is the default.

PIPE
List the amount of data left unacknowledged.

STATE
List the beginning and ending state of each session.

SUMMARY
Show only the summary statistics.

Tip: The UDP session analysis is also used for other protocols.

SITELOCAL
Select packets with an IPv6 site-local unicast address prefix. Equivalent to IPADDR(FEC0::/10).

SMC
This packet was sent across Shared Memory Communications.

SMCLLC
Select packets with a protocol number of 252 for Shared Memory Communications over Remote Direct Memory Access (SMC-R). Equivalent to PROTOCOL(252).

SMTP[(port_number|25)]
Select SMTP protocol packets. The port_number defines the SMTP port number to select packets for formatting. Equivalent to PORT(25).

SNIFFER[(*nnnnn*|200, ETHERNET|TCPDUMP)]
Writes the trace records in a format acceptable for downloading to other trace analysis programs, such as programs from http://www.tcpdump.org/.

nnnnn
The maximum size of trace data. Packets with more data than this value are truncated. The default is 200 bytes. The largest value is derived from the LRECL of the SNIFFER data set.

ETHERNET
If this keyword is specified, the output is formatted for the Ethernet analysis application of the analyzer. This keyword specifies the file format only and does not imply that only packets traced on an Ethernet are collected. Packets from all devices can be collected by using this option.

The default for the SNIFFER option is ETHERNET.

TCPDUMP
The format is compatible with the files with an Ethernet header.

Note: The TOKENRING keyword on the CTRACE OPTIONS((SNIFFER(TOKENRING))) on the IPCS CTRACE subcommand is ignored. The ETHERNET format of the sniffer data set is selected.

The trace records are written to the file with a DD name of SNIFFER. After the file is generated, it can be downloaded as a binary file to the analyzer and loaded by using the standard features of the analyzer. Use NOREASSEMBLY to prevent the formatter from reassembling packets. Then, each packet is passed as the packets are collected. The logical record length of the SNIFFER data set determines the largest amount of packet data that is written to the data set.

Allocate a file with DDNAME of SNIFFER before you invoke the CTRACE command with SNIFFER in the OPTIONS string as follows:

```
ALLOC FILE(SNIFFER)
DA(PACKET.TRC) SPACE(15 15) TRACK +
                      LRECL(8000) BLKSIZE(32000)
```

The data set has a record format of variable blocked with a logical record length of 8000 bytes. The maximum IP packet size is 7962 (8000 - 38) for SNIFFER(ETHERNET).

The minimum logical record length of the data set is 256 bytes.

Restriction: Do not use the SNIFFER option when the CTRACE subcommands are used with the IPCS MERGE subcommand. The SNIFFER data file is written over by the multiple CTRACE commands that specify the SNIFFER option.

SNMP[(port_number|161 port_number|162)]
Select SNMP protocol packets. The port_number defines the SNMP port number to select packets for formatting. Equivalent to PORT(161 162).

SPEED(local|10,remote|10)
The link speed, in megabits per second, for the local and remote link. These values are used in throughput calculations in the TCP session report. Valid values are in the range 0 - 17171. The default value is 10. Specify the slowest speed of the link in the route.

STATISTICS[(DETAIL|SUMMARY)]
After all the records are processed, generate statistical reports.

DETAIL
Reports are produced showing the number of records that are selected by

record type, device type, job name, link name, protocol number, IP address and port numbers. The session summary report is a listing of the IP address and port number pairs that shows the number of records, the first and last record numbers, and the first and last record times.

SUMMARY
Only the session summary report is produced. SUMMARY is the default.

TALLY on the CTRACE command selects this option if no other report options are specified.

STATS
Equivalent to the STATISTICS option.

STREAMS[(stream_size|128 DETAIL|SUMMARY)]
Collect the packet data for dumping or formatting after the trace file is processed. The value *nnn* represents the maximum amount of storage that is used to capture each stream. The value *stream_size* represents the maximum amount of storage that is used to capture each stream. The smallest value is 16 KB. The largest value is 512 KB. The default value is 128 KB. The value is in 1024 bytes (1K) units.

SUMMARY
List about each packet in the stream. SUMMARY is the default.

DETAIL
Issue messages about the status of the stream.

Requirement: The DUMP keyword is required to dump the packet data.

SUBAREA(subarea_number_list)
Select SNA protocol packets with a matching subarea address in the TH4 transmission header. Valid values are in the range 1 - 65535. You can specify up to 16 subarea numbers.

SUMMARY
Format a single line for each trace record. SUMMARY on the CTRACE command selects this option if no other report options are specified. If no other report option specified on the CTRACE command, then SUMMARY is selected as the report.

NOTOD
Use the time that the trace data was moved to the CTRACE buffers for the reports. Normally, the time that the trace data was moved to the trace buffer is shown. The CTRACE command uses the time stamp when the trace data was moved to the buffers for START and STOP time selection. NOTOD is the default value for SYSTCPDA and SYSTCPIS traces.

TOD
Use the time that the trace data was captured for the reports. Normally, the time that the trace data was moved to the trace buffer is shown. The CTRACE command uses the time stamp when the trace data was moved to the buffers for START and STOP time selection. TOD is the default value for SYSTCPOT traces, which uses the time stamp that is generated by the OSA trace function.

TALLY
Equivalent to the STATISTICS(DETAIL) option.

TCID(transport connection_id_list)
Select SNA protocol packets with a matching transport connection identifier in

the RTP transport header. Valid values include 1 - 16 hexadecimal digits. Up to 16 transport connection identifiers can be specified.

TCP
Select packets with a protocol number of 6. Equivalent to PROTOCOL(6).

TELNET[(port_number|23 [screen_width|80] [SUMMARY|DETAIL])]
Select TELNET protocol packets. The port_number defines the TELNET port number to select packets for formatting. Equivalent to PORT(23).

The screen_width parameter defines the value that is used for converting buffer offsets into row and column values for the 3270 data stream formatting. If the screen_width parameter is provided, then the port_number parameter must also be used. The minimum value is 80. The maximum value is 255. The default value is 80.

SUMMARY formats the 3270 data stream into a representation of the screen.

DETAIL formats each 3270 command and order.

There is no default for DETAIL or SUMMARY.

TFTP[(port_number|69)]
Select TFTP protocol packets. The port_number defines the TFTP port number to select packets for formatting. Equivalent to PORT(69).

TH5ADDR(session_address_list)
Select SNA protocol packets with a matching session address in the TH5 transmission header. Valid values include 1 - 16 hexadecimal digits. You can specify up to 16 session addresses.

TIME[(port_number|37)]
Select TIME protocol packets. The port_number defines the TIME port number to select packets for formatting.

TRAFFICCLASS(traffic_class)
Select the records with the matching IPv6 traffic class field. Up to 16 traffic class values can be specified in the range from 0 to 255. Each entry in the list can be a range: `low_number:high_number`. Values can be decimal (nn) or Hexadecimal (X'hh').

UDP
Select packets with a protocol number of 17. Equivalent to PROTOCOL(17).

USEREXIT(exitname)
Names the user exit to be called for each selected record. The USEREXIT keyword on the CTRACE command names a user exit that is called before the SYSTCPDA packet trace filtering is done. If this exit routine returns a nonzero return code, then the record is skipped by the SYSTCPDA formatter.

VLANID(*vlanid*)
Select packets that are written to or received from an OSAENTA trace with one of the specified VLAN identifiers. From 1 to 16 identifiers can be specified. This filter applies only to type 7 trace records. A VLAN identifier has a value in the range 0 - 4094.

Tip: The DEVICEID, MACADDR, ETHTYPE, and VLANID filter keywords apply to SYSTCPOT data. If these keywords are specified with SYSTCPDA data, then these filters are ignored.

WWW[(port_number|80)]
Select HTTP protocol packets. The port_number defines the HTTP port number to select packets for formatting. Equivalent to PORT(80).

X25
Select packet trace records created by the X25 processor.

Tip: This option is obsolete, but it is still accepted.

Diagnosing problems with Shared Memory Communications

Shared Memory Communications (SMC) problems are often related to switch configuration, VLAN connectivity, physical network ID (PNetID) configuration, and other configuration issues.

Common problems with using SMC include the following categories:

- "SMC-R switch configuration issues"
- "SMC-R VLAN configuration issues" on page 221
- "SMC-D VLAN connectivity issues" on page 222
- "Physical network ID configuration issues" on page 222
- "No associated subnet mask" on page 223
- "PFID status remains STARTING" on page 224
- "Problem with SMC interaction with security function" on page 224

The SMCReason field of the Netstat ALL/-A report and the SMCR or SMCD field of the Netstat DEvlinks/-d report provide information that is related to SMC problems. The SMCR field applies to Shared Memory Communications over Remote Direct Memory Access (SMC-R) processing, and the SMCD field applies to Shared Memory Communications - Direct Memory Access (SMC-D) processing.

For a complete list of SMCReason codes in the Netstat ALL/-A report and the SMCR or SMCD Disabled reasons in the Netstat DEvlinks/-d report, see z/OS Communications Server: IP System Administrator's Commands.

SMC-R switch configuration issues

Remote Direct Memory Access (RDMA) processing requires standard 10GbE switch support, and distance limitations might exist. Enable the global pause frame (a standard Ethernet switch feature for Ethernet flow control that is described in the IEEE 802.3x standard) on the switch.

When the SMCReason field of the Netstat ALL/-A report is 00005013 - RDMA CONNECTIVITY FAILURE, VTAM was not able to complete the SMC-R Link Confirm flow, which usually indicates a switch configuration issue. The Link Confirm message is the first data sent over the RDMA over Converged Ethernet (RoCE) fabric. Check for the following issues:

- If you are using VLANs, verify that the VLAN configuration on the RoCE switch ports is consistent with the VLAN configuration on the OSD switch ports.

  For example, the OSD switch ports might be configured properly, with no VLAN ID or the default VLAN ID, but the RoCE switch ports have a different VLAN ID configured, such as trunk mode with VLAN IDs 400® and 500.

  For more information about configuring VLANs with SMC-R, see "SMC-R VLAN configuration issues" on page 221.
- Verify that your cable is plugged into the correct port on the IBM 10GbE RoCE Express feature and into the correct port on the switch.

For example, the cable might be plugged into the correct port on the 10GbE RoCE Express feature but into the wrong port on the switch, or the cable might be plugged into the correct port on the switch but into the wrong port on the 10GbE RoCE Express feature.

- Verify that the MTU value configured on the switch is large enough to support your configured MTU size on GLOBALTCPIP SMCR MTU for this interface.

  Enable jumbo frame support on the RoCE switch ports.
- Multiple switches are in use but the switch uplinks are not configured properly.
- For some switches (for example the IBM RackSwitch G8264), you might need to configure the RoCE switch ports as edge ports. This places the port in the forwarding state as soon as the link is up, reducing delays due to Spanning Tree Protocol processing.

Verify that you have Ethernet flow control enabled on your switch. Ethernet flow control is implemented by using pause frames. If the control is not enabled, this can cause the switch to be overrun leading to packet loss.

SMC-R VLAN configuration issues

The SMC-R VLAN configuration checklist is provided for you to verify that your VLAN environment for RoCE, and therefore for SMC-R, is correctly configured.

1. Verify the consistency of the VLAN mode settings for your Ethernet switch port.

   The VLAN mode setting for an Ethernet switch port can be access mode or trunk mode. The VLAN mode for the Ethernet switch port for an OSA Express port must be the same VLAN mode for the Ethernet switch port for the associated IBM 10GbE RoCE Express ports. For example, if the Ethernet switch ports for the OSA Express are configured in access mode, the Ethernet switch ports for their associated IBM 10GbE RoCE Express ports must also be configured in access mode.
2. Verify the consistency of the VLAN access that is available to Ethernet switch ports that IBM 10GbE RoCE Express features use.

   All IBM 10GbE Express ports for a specific physical network ID (PNetID) must have access to the same VLANID value:

   - If you use access mode, only a single VLANID can be used, and all Ethernet switch ports that serve the IBM 10GbE RoCE Express ports for a specific PNetID must be configured with this single VLANID. This VLANID is not required to match any of the VLANIDs that are configured for the Ethernet switch ports that serve the associated OSA Express features.
   - If you use trunk mode, all Ethernet switch ports that serve the IBM 10GbE RoCE Express ports for a specific PNetID must be configured with the same set of VLANID values as the Ethernet switch ports that serve the associated OSA Express features.
3. Verify VLAN mode consistency across all z/OS hosts that use SMC-R for a specific PNetID.

   All z/OS hosts that connect to the same PNetID for SMC-R communication must use the same VLAN mode, either access mode or trunk mode. You cannot mix access mode and trunk mode among the z/OS hosts for the same PNetID.

Guideline: The IBM 10GbE RoCE Express feature inherits the VLANID from the OSA interfaces within the same physical network. You do not specifically configure a VLANID for the IBM 10GbE RoCE Express feature.

For more information about configuring VLANs with SMC-R, see SMC-R VLAN configuration considerations in Shared Memory Communications over RDMA Reference Information (http://www-01.ibm.com/software/network/commserver/SMCR/).

For more information about VLAN support with SMC, see VLANID considerations in z/OS Communications Server: IP Configuration Guide.

SMC-D VLAN connectivity issues

Internal shared memory (ISM) processing does not require network switches. However, VLANs are supported over ISM devices to allow for separation of traffic. The OSD or HiperSockets VLAN attributes propagate to the associated ISM interfaces that use the same physical network ID (PNetID).

No additional HCD definition is required to identify VLANID values that an ISM device can use. During activation processing, VTAM registers with the ISM device the VLANIDs that the ISM interfaces use.

If you are using VLANs, ensure the compatibility of VLANID values on the OSD or HiperSockets interfaces that are used to establish the TCP connection. If a mismatch between VLANID values occurs, the SMCReason field of the Netstat ALL/-A report indicates `00005806 — VLAN ID NOT FOUND`.

For more information about configuring VLANs with SMC-D, see VLANID considerations in z/OS Communications Server: IP Configuration Guide.

Physical network ID configuration issues

The TCP/IP stack must be able to determine which physical network is connected to a particular 10GbE RoCE Express or internal shared memory (ISM) interface, so that the 10GbE RoCE Express or ISM interface can be associated with the SMC capable interfaces that connect to that same physical network.

- For Shared Memory Communications over Remote Direct Memory Access (SMC-R), SMC capable interfaces include IPAQENET and IPAQENET6 interfaces.
- For Shared Memory Communications - Direct Memory Access (SMC-D), SMC capable interfaces include IPAQENET, IPAQENET6, IPAQIDIO, and IPAQIDIO6 interfaces.

SMC-R physical network ID configuration issues

Use the Netstat DEvlinks/-d and D NET,TRL,TRLE=xxxx commands to verify the physical network ID (PNetID) value on the OSD interfaces and the 10GbE RoCE Express interfaces.

- If the Netstat DEvlinks/-d report for your OSD interface indicates SMCR: DISABLED (NO PNETID), ensure that you configured the PNetID value on the correct OSD port in the HCD definitions.
- If you receive message EZD2028I with reason PNETID IS NOT CONFIGURED during 10GbE RoCE Express interface activation, ensure that you configured the PNetID value on the correct 10GbE RoCE Express port in the HCD definitions.
- If the Netstat DEvlinks/-d report for your OSD interface indicates SMCR: Yes and your 10GbE RoCE Express interfaces initialized successfully, verify that the PNetID value of the OSD interface matches that of the intended 10GbE RoCE Express interfaces.

In the HCD definitions, value PNetID 1 is for port 1 on 10GbE RoCE Express features and port 0 on OSD adapters, and value PNetID 2 is for port 2 on 10GbE RoCE Express features and port 1 on OSD adapters. Values PNetID 3 and PNetID 4 are not used.

For more information about configuring PNetIDs, see Physical network considerations in z/OS Communications Server: IP Configuration Guide.

SMC-D physical network ID configuration issues

Use the Netstat DEvlinks/-d and D NET,TRL,TRLE=xxxx commands to verify the physical network ID (PNetID) value on the OSD or HiperSockets interfaces and the ISM interfaces.

- If the Netstat DEvlinks/-d report for your OSD or HiperSockets interface indicates SMCD: DISABLED (NO PNETID), ensure that you configured the PNetID value on the correct OSD port or HiperSockets CHPID in the HCD definitions.
- During ISM interface activation, if you receive message EZD2028I with reason PNETID IS NOT CONFIGURED or message IST2422I, ensure that you configured the PNetID value on the correct ISM device in the HCD definitions.
- During ISM interface activation, if you receive message IST2423I, ensure that you have configured sufficient Peripheral Component Interconnect Express (PCIe) function ID (PFID) values for the PNetID value in the HCD definitions.
- If the Netstat DEvlinks/-d report for your OSD or HiperSockets interface indicates SMCD: Yes and your ISM interfaces initialized successfully, verify that the PNetID value of the OSD or HiperSockets interface matches the PNetID of the intended ISM interfaces.

In the HCD definitions, the same PNetID values have different meaning for different types of devices.

Device type	PNetID 1	PNetID 2	PNetID 3	PNetID 4
ISM device	Represents the device	Not used	Not used	Not used
OSD adapter	Represents port 0	Represents port 1	Not used	Not used
HiperSockets device	Represents the device	Not used	Not used	Not used

For more information about configuring PNetIDs, see Physical network considerations in z/OS Communications Server: IP Configuration Guide.

No associated subnet mask

Shared Memory Communications (SMC) is used only between peers whose IPv4 interfaces have the same subnet value or whose IPv6 interfaces have at least one prefix in common.

- For IPv4, if the SMCR or SMCD field of the Netstat DEvlinks/-d report for an OSD interface is DISABLED (NO SUBNET MASK), it means no subnet mask value is configured for the OSD interface.
- For IPv4, if the SMCD field of the Netstat DEvlinks/-d report for a HiperSockets interface is DISABLED (NO SUBNET MASK), it means no subnet mask value is configured for the HiperSockets interface.

- For IPv4, if the SMCReason code in the Netstat ALL/-A report is 521E PEER SUBNET/PREFIX MISMATCH, the interfaces on the peer stacks use different subnets.
- For IPv6, if the SMCReason code in the Netstat ALL/-A report is 521E PEER SUBNET/PREFIX MISMATCH, the interfaces on the peer stacks do not have a prefix in common.

For information about associating your interfaces with the appropriate subnet or prefix, see Configuring Shared Memory Communications over RDMA and Configuring Shared Memory Communications - Direct Memory Access in z/OS Communications Server: IP Configuration Guide.

PFID status remains STARTING

The PFIDSTATUS field is the Peripheral Component Interconnect Express® (PCIe) function ID (PFID) status for the RNIC or the internal shared memory (ISM) interface.

The following list describes the possible status values:

- READY

  READY indicates that the initialization sequence with the PFID is complete and the PFID is ready.
- NOT ACTIVE

  NOT ACTIVE indicates that the PFID was never started or was stopped after it was started.
- STARTING

  STARTING indicates that a START of the PFID was issued and TCP/IP sent an activation request to the Data Link Control (DLC) layer.

  For an ISM interface, this should be a transitory state.

  For an RNIC interface, if the PFIDSTATUS remains STARTING, this means z/OS Communications Server did not receive a port state change event that indicates the port is active from the 10GbE RoCE Express feature. Until the port state change event is received, the PFIDSTATUS remains in STARTING state.

  Take the following actions if the PFIDSTATUS field does not change from STARTING to READY for an RNIC interface:
  - Check that your cables are connected properly.
  - Verify that the switch ports are enabled.
  - If the RoCE adapters are hard-wired to each other, the STARTING status is expected until the partner side has started the RNIC interface.
  - Verify that the optical cable used for the RoCE adapter is not damaged.

Problem with SMC interaction with security function

Generally, security functions that require TCP/IP to examine TCP packets cannot be used with SMC communications because data that is sent over SMC links is not converted into TCP packets.

For more information, see Security functions in z/OS Communications Server: IP Configuration Guide.

Chapter 6. IP System Administrator's Commands

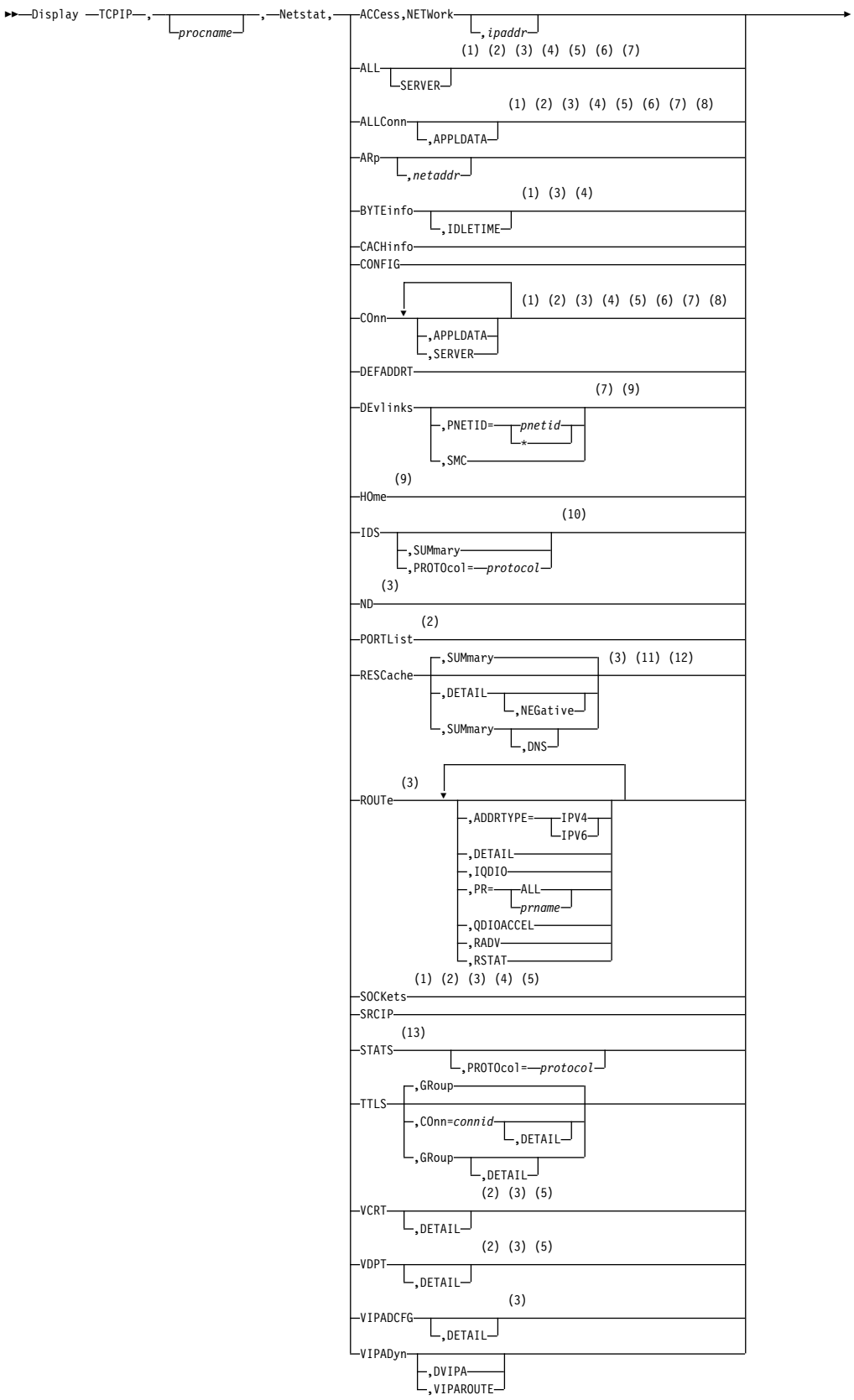
DISPLAY TCPIP,,NETSTAT

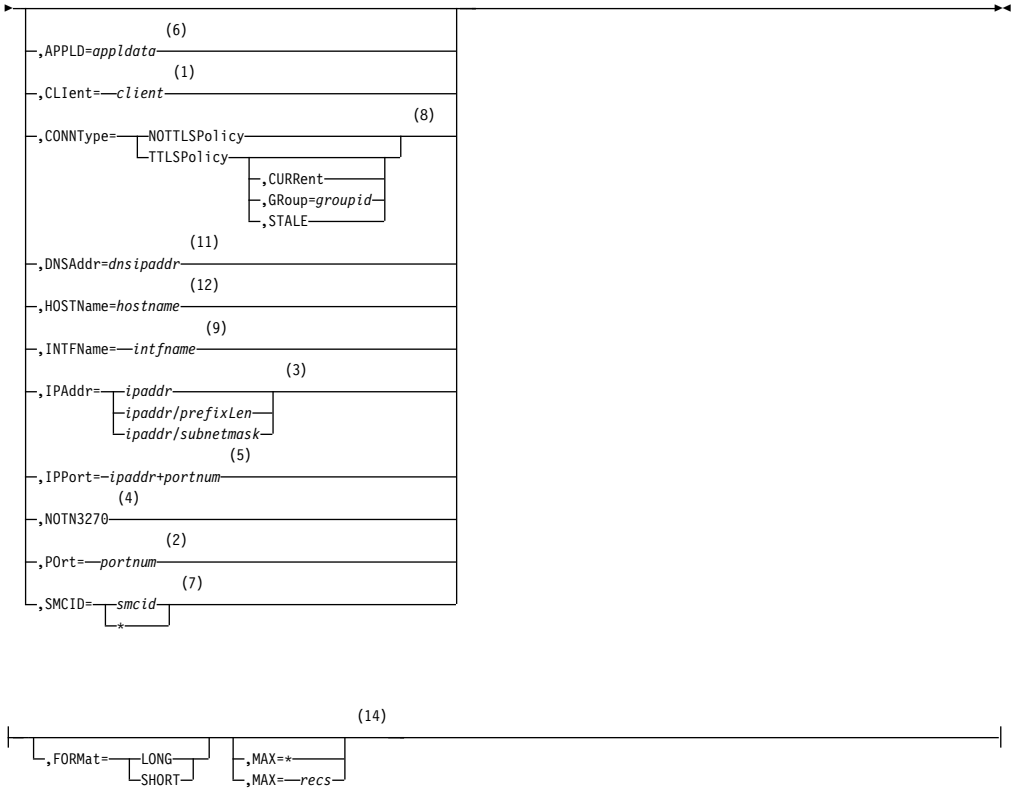
Use the DISPLAY TCPIP,,NETSTAT command from an operator console to request Netstat information. For a detailed description of each report, see Netstat report details and examples. This command can display only 65 533 lines of output for each report. If the command cannot display all of the report output, the report is truncated and the END OF THE REPORT output line is not displayed. Instead, the following output line is displayed at the end of the report:

```
REPORT TRUNCATED DUE TO GREATER THAN 65533 LINES OF OUTPUT
```

You can use the MAX parameter or filter parameters to limit the number of records that are displayed for a report.

Format


Display TCPIP, procname, Netstat,
ACCess,NETWork ,ipaddr
(1) (2) (3) (4) (5) (6) (7)
ALL SERVER
(1) (2) (3) (4) (5) (6) (7) (8)
ALLConn ,APPLDATA
ARp ,netaddr
(1) (3) (4)
BYTEinfo ,IDLETIME
CACHinfo
CONFIG
(1) (2) (3) (4) (5) (6) (7) (8)
COnn ,APPLDATA ,SERVER
DEFADDRT
(7) (9)
DEvlinks ,PNETID= pnetid * ,SMC
(9)
HOme
(10)
IDS ,SUMmary ,PROTOcol= protocol
(3)
ND
(2)
PORTList
,SUMmary (3) (11) (12)
RESCache ,DETAIL ,NEGative
,SUMmary ,DNS
(3)
ROUTe ,ADDRTYPE= IPV4 IPV6 ,DETAIL ,IQDIO ,PR= ALL prname ,QDIOACCEL ,RADV ,RSTAT
(1) (2) (3) (4) (5)
SOCKets
SRCIP
(13)
STATS ,PROTOcol= protocol
,GRoup
TTLS ,COnn=connid ,DETAIL
,GRoup ,DETAIL
(2) (3) (5)
VCRT ,DETAIL
(2) (3) (5)
VDPT ,DETAIL
(3)
VIPADCFG ,DETAIL
VIPADyn ,DVIPA ,VIPAROUTE



Notes:

1 The CLIent filter is valid only with ALL, ALLConn, BYTEinfo, COnn, and SOCKets.

2 The POrt filter is valid only with ALL, ALLConn, COnn, PORTList, SOCKets, VCRT, and VDPT.

3 The IPAddr filter is valid only with ALL, ALLConn, BYTEinfo, COnn, ND, RESCache, ROUTe, SOCKets, VCRT, VDPT, and VIPADCFG.

4 The NOTN3270 filter is valid only with ALL, ALLConn, BYTEinfo, COnn, and SOCKets.

5 The IPPort filter is valid only with ALL, ALLConn, COnn, SOCKets, VCRT, and VDPT.

6 The APPLD filter is valid only with ALL, ALLConn, and COnn.

7 The SMCID filter is valid only with ALL, ALLConn, COnn, and DEvlinks.

8 The CONNType filter is valid only with ALLConn and COnn.

9 The INTFName filter is valid only with DEvlinks and HOme.

10 The valid protocol values are TCP and UDP.

11 The DNSAddr select string is valid only with RESCache.

12 The HOSTName select string is valid only with RESCache.

13 The valid protocol values are IP, ICMP, TCP, and UDP.

14 If the MAX parameter is not specified on the command, the default value for the MAX parameter is the value of the MAXRECS parameter on the GLOBALCONFIG profile statement.

Parameters

Note: The minimum abbreviation for each parameter is shown in uppercase letters.

Netstat
Request NETSTAT information.

ACCess,NETWork
Displays information about the network access tree in TCP/IP.

ALL
Displays detailed information about TCP connections and UDP sockets, including some that were recently closed.

SERVER
Provides detailed information only for TCP connections that are in the listen state.

ALLConn
Displays information for all TCP/IP connections, including recently closed ones.

APPLDATA
Displays application data in the output report.

ARp
Displays ARP cache information.

netaddr
This field has a maximum length of 15. Format is *nnn.nnn.nnn.nnn* where *nnn* is in the range 0 - 255. You must code all the triplets. No wildcards are allowed.

BYTEinfo
Displays the byte-count information about each active TCP connection and UDP socket. At the end of the report, the number of records written and the total number of records are displayed. The total number of records represents all UDP sockets and all TCP connections, not just active TCP connections.

IDLETIME
Displays the idle time for each connection.

CACHinfo
Displays information about Fast Response Cache Accelerator statistics. Statistics are displayed for each listening socket configured for Fast Response Cache Accelerator support. There is one section displayed per socket.

CONFIG
Displays TCP/IP configuration data.

COnn
Displays information about each active TCP/IP connection. At the end of the report, the number of records written and the total number of records are displayed. The total number of records represents all UDP sockets and all TCP connections, not just active TCP connections.

APPLDATA
Displays application data in the output report.

SERVER
Displays detailed information about TCP connections in the listen state.

DEFADDRT
Displays the policy table for IPv6 default address selection.

DEvlinks
Displays information about interfaces in the TCP/IP address space.

PNETID=*pnetid*
Displays information about interfaces for the specified physical network ID (*pnetid*). If an asterisk (*) is specified for the PNETID value, all interfaces with a PNETID are displayed. This modifier is mutually exclusive with the SMC modifier.

SMC
Displays only Shared Memory Communications (SMC) information.

- For Shared Memory Communications over Remote Direct Memory Access (SMC-R), displays information only about RDMA network interface card (RNIC) interfaces and their associated SMC-R link groups and SMC-R links.
- For Shared Memory Communications - Direct Memory Access (SMC-D), displays information only about Internal Shared Memory (ISM) interfaces and their associated SMC-D links.

This modifier is mutually exclusive with the PNETID modifier.

Tip: If the INTFName/-K filter is specified with the SMC modifier, the SMC-R link group information is not displayed.

HOme
Displays the home list.

IDS
Displays information about intrusion detection services.

SUMmary
Displays summary information about intrusion detection services.

PROTOcol=*protocol*
Displays information about intrusion detection services for the specified *protocol*. The valid protocols are TCP and UDP.

ND Displays IPv6 Neighbor Discovery cache information.

PORTList
Displays the list of reserved ports and the port access control configuration for unreserved ports. Configure port access control for unreserved ports by specifying PORT profile statements with the port number value replaced by the keyword UNRSV. For more information about port access control, see port access control information in z/OS Communications Server: IP Configuration Guide.

For ports that are reserved by the PORTRANGE profile statement, only one output line is displayed for each range.

RESCache
Displays information about the operation of the system-wide resolver cache. This information is not specific to the TCP/IP stack whose name was specified on the D TCPIP command. Statistical information, such as number of record entries or number of cache queries, can be retrieved, or detailed information about some or all of the cache entries can be retrieved. Resolver caching is configured using resolver configuration statements in the resolver setup file.

For more information about resolver caching, see details about resolver caching in z/OS Communications Server: IP Configuration Guide.

DETAIL
Display detailed information for all unexpired entries that are currently in the resolver cache. This information can include the following contents:

- Host-name-to-IP address entries from resolver forward lookups
- IP-address-to-host-name entries from resolver reverse lookups
- Negative entries included in both forward and reverse lookup tables

NEGative
Display detailed information for all negative cache entries in the resolver cache.

SUMmary
Display general system statistics for resolver cache operations. This is the default report for the RESCACHE report option.

DNS
Display general system statistics for resolver cache operations, plus individual statistics for each DNS name server that has provided information that is currently stored in the cache.

Result: Using the DETAIL modifier might cause a large amount of data to be displayed from the MVS console. As an alternative, consider using either the z/OS UNIX shell or TSO version of the command when you have large amount of resolver cache information.

ROUTe
Displays routing information. For a complete description of ROUTe, see Netstat ROUTe/-r report.

Note: Static routes over deleted interfaces are removed from the main routing table and therefore do not appear in the reports generated for the main routing table. Loopback routes are displayed as well as implicit (HOME list) routes.

ADDRTYPE
Displays routing information.

IPV4
Displays IPv4 routing information. This parameter is mutually exclusive with the RADV parameter.

IPV6
Displays IPv6 routing information.

DETAIL
Displays the preceding information plus the metric or cost of use for the route, and displays the following MVS-specific configured parameters for each route:

- Maximum retransmit time
- Minimum retransmit time
- Round-trip gain
- Variance gain
- Variance multiplier

This parameter is mutually exclusive with the QDIOACCEL and IQDIO parameters.

PR
Displays policy-based routing tables. This parameter is mutually exclusive with the QDIOACCEL and IQDIO parameters.

ALL
Displays all policy-based routing tables.

prname
Displays the policy-based routing table that has the name *prname*.

Restriction: Only active policy-based routing tables can be displayed with the Netstat ROUTe command. A policy-based routing table is active if an active routing rule and its associated action reference the policy-based routing table. You can display both active and inactive policy-based routing tables by using the **pasearch** command. For more information, see The z/OS UNIX pasearch command: Display policies.

QDIOACCEL
IQDIO
Displays routes that are eligible for accelerated routing by using the QDIO Accelerator or HiperSockets Accelerator. See information about QDIO Accelerator and efficient routing using HiperSockets Accelerator in z/OS Communications Server: IP Configuration Guide for more details. This parameter is mutually exclusive with the DETAIL, PR, RADV, and RSTAT parameters.

RADV
Displays all of the IPv6 routes that are added based on information received in router advertisement messages. All IPv6 router advertisement routes are displayed regardless of whether they are currently used for routing. The flags and reference count are not displayed on the report. This parameter is mutually exclusive with the RSTAT, QDIOACCEL, IQDIO, and ADDRTYPE=IPV4 parameters.

RSTAT
Displays all of the static routes that are defined as replaceable. All defined replaceable static routes are displayed without regard to whether they are currently being used for routing. The flags and reference count are not displayed on the report. The MTU value that is displayed in this report is the value that was defined by using the MTU parameter in the ROUTE statement, or the default value for the specified interface type. This parameter is mutually exclusive with the RADV, QDIOACCEL, and IQDIO parameters.

SOCKets
Displays information for open TCP or UDP sockets that are associated with a client name.

SRCIP
Displays information for all job-specific and destination-specific source IP address associations on the TCP/IP address space.

STATS
Displays TCP/IP statistics for each protocol.

PROTOcol=*protocol*
Displays statistics for the specified protocol. The valid protocols are IP, ICMP, TCP, and UDP.

Result: If you specify TCP, you get TCP, SMC-R, and SMC-D statistics.

TTLS
Displays Application Transparent Transport Layer Security (AT-TLS) information for TCP protocol connections.

COnn=*connid*
Displays the name of the AT-TLS policy rule and the names of the associated actions for the specified connection. The specified *connid* is a number assigned by the TCP/IP stack to uniquely identify a socket entity. You can determine the *connid* from the Conn column in the "Netstat ALLConn/-a report" on page 300.

DETAIL
Displays the AT-TLS policy rule and the associated actions for the specified connection.

GRoup
Displays summary information for AT-TLS groups. AT-TLS groups are defined using the TTLSGroupAction policy statement. The AT-TLS group exists as long as the TTLSGroupAction statement is current or as long as there are active connections using the group.

DETAIL
Displays detailed information for AT-TLS groups.

VCRT
Displays the dynamic VIPA Connection Routing Table information.

DETAIL
For each entry that represents an established dynamic VIPA connection or an affinity created by the passive-mode FTP, displays the preceding information plus the policy rule, action information, routing information, and acceleration information.

For each entry that represents an affinity created by the TIMEDAFFINITY parameter on the VIPADISTRIBUTE profile statement, displays the preceding information plus the affinity related information.

VDPT
Displays the dynamic VIPA Destination Port Table information.

DETAIL
If this optional keyword is specified, when the table for TCP/IP stacks is displayed, the output contains policy action information, target responsiveness values, and a Workload Manager weight value (W/Q), on a separate line. If the DETAIL keyword is not specified, the output does not contain this information.

When the table for non-z/OS targets is displayed, the output contains the weight of the non-z/OS target. If the DETAIL keyword is not specified, the output does not contain this information.

VIPADCFG
Displays the current dynamic VIPA configuration information for a host.

VIPADyn
Displays the current dynamic VIPA and VIPAROUTE information for a local host.

DVIPA
Displays the current dynamic VIPA information only.

VIPAROUTE
Displays the current VIPAROUTE information only.

APPLD=*appldata*
Filter the output of the ALL, ALLConn, and COnn reports by using the specified application data appldata. The maximum size for this field is 40 alphanumeric characters.

CLIent=*client*
Specifies a client name that is used to limit the ALL, ALLConn, BYTEinfo, COnn, and SOCKets responses. Maximum size for this field is 8 alphanumeric characters (plus special characters #, $, and @). Wildcards (* and ?) can appear in any position.

CONNType
Specifies a connection type to limit the ALLConn and COnn responses.

NOTTLSPolicy
Displays only those connections that have not been matched to an Application Transparent Transport Layer Security (AT-TLS) rule. This includes connections that were established while the AT-TLS function was disabled (NOTTLS is specified or in effect by default on the TCPCONFIG statement) and all connections that are not using the TCP protocol. For TCP connections that were established while the AT-TLS function was enabled, this includes the following connections:

- Connections for which AT-TLS policy lookup has not yet occurred (typically the first send or receive has not yet been issued).
- Connections for which AT-TLS policy lookup has occurred but for which no matching rule was found.

TTLSPolicy
Displays only connections that match an Application Transparent Transport Layer Security (AT-TLS) rule. This includes only connections that were established while the AT-TLS function was enabled, for which an AT-TLS policy rule was found with the value `TTLSEnabled ON` or `TTLSEnabled OFF` specified in the TTLSGroupAction. Responses can be further limited on AT-TLS connection type. AT-TLS connection type has the following values:

CURRent
Displays only connections that are using AT-TLS where the rule and all actions are still available to be used for new connections.

GRoup=*groupid*
Displays only connections that are using the AT-TLS group specified by the *groupid* value. The specified *groupid* value is a number assigned by the TCP/IP stack to uniquely identify an AT-TLS group. You can determine the *groupid* value from the GroupID field in the Netstat TTLS GROUP report.

STALE
Displays only connections that are using AT-TLS where the rule or at least one action is no longer available to be used for new connections.

DNSAddr=*dnsipaddr*
Filter the output of the RESCache report using the specified DNS IP address *dnsipaddr*.

HOSTName=*hostname*
Filter the output of the RESCache report using the specified host name value *hostname*.

INTFName=*intfname*

Specifies a name that you can use to limit the DEvlinks and HOme report options to a single interface or to a group of interfaces.

For the DEvlinks and HOme report options, the INTFName filter can be one of the following values:

- The link name of a network interface that was configured on a LINK profile statement (this option selects one interface).
- The interface name of a network interface that was configured on an INTERFACE profile statement (this option selects one interface).
- The port name of an OSA-Express feature in QDIO mode. This is the name that is specified on the PORTNAME keyword in the TRLE (this option selects all interfaces that are associated with the OSA-Express port, including an OSAENTA trace interface).
- The name of a HiperSockets TRLE (this option selects all interfaces that are associated with the HiperSockets TRLE).

Additionally, for the DEvlinks report option, the INTFName filter can also be the interface name of an OSAENTA trace interface, which is EZANTA*portname*, where the *portname* value is the name that is specified on the PORTNAME keyword in the TRLE for the OSA-Express port that is being traced (this option selects one interface). The INTFName filter is not supported for the DEvlinks report if the PNETID modifier is specified.

IPAddr

Provides the option response on specified *ipaddr*, *ipaddr/subnetmask* or *ipaddr/prefixlength*

ipaddr Provides the response for ALL, ALLConn, BYTEinfo, COnn, ND, RESCache, ROUTe, SOCKets, VCRT, and VDPT on the specified IP address (*ipaddr*). Except for the RESCache option, with IPv4 addresses, the default subnet mask 255.255.255.255 is used; for IPv6 addresses, the default prefix length 128 is used. The RECache option does not support any default subnet mask or default prefix length.

ipaddr/subnetmask

Provides the response for ALL, ALLConn, BYTEinfo, COnn, ROUTe, SOCKets, VCRT, and VDPT on the specified IP address with specified subnet mask (*ipaddr/subnetmask*). The IP address (*ipaddr*) in this format must be an IPv4 IP address.

ipaddr/prefixlength

Provides the response for ALL, ALLConn, BYTEinfo, COnn, ND, ROUTe, SOCKets, VCRT, and VDPT on the specified IP address and prefix length. For IPv4 addresses, the prefix length range is 1 - 32. For IPv6 addresses, the prefix length range is 1 - 128.

IPPort=*ipaddr***+***portnum*

Specifies the IP address and port that are used to limit the ALL, ALLConn, COnn, SOCKets, VCRT, and VDPT report options to the TCP local endpoints, TCP remote endpoints, or the UDP local endpoint. The specified IPv4 *ipaddr* value can be up to 15 characters in length, denoting a single IPv4 IP address; the specified IPv6 *ipaddr* value can be up to 45 characters in length, denoting a single IPv6 IP address. For TCP, the filter values *ipaddr* and *portnum* match any combination of the local and remote IP address and local and remote port.

NOTN3270

Provides the response of ALL, ALLConn, BYTEinfo, COnn, and SOCKets, excluding TN3270E Telnet server connections.

POrt=*portnum*
Specifies a port that is used to limit the ALL, ALLConn, COnn, PORTList, SOCKets, VCRT, and VDPT options. The port value range, for all options except the PORTLIST option, is 0 - 65535. No wildcards are allowed. For the PORTList option only, the port value range is 1 - 65535 and you can also filter on the keyword UNRSV.

SMCID=*smcid*
Specifies a Shared Memory Communications identifier that is used to limit the ALL, ALLConn, COnn, and DEvlinks report options. The identifier can represent an SMC-R link, SMC-R link group, or SMC-D link. If an asterisk (*) is specified for the filter value, Netstat provides output only for entries that are associated with SMC-R links, SMC-R link groups, and SMC-D links. The SMCID filter is not supported for the DEvlinks report if the PNETID modifier is specified.

MAX=*recs*
The maximum number of records for which Netstat displays information on the console. The value *recs* indicates the number of records that are displayed on each report. For example, for the connection-related reports, a record is a TCP connection or listener, or a UDP endpoint. Valid *recs* values are in the range 1 - 65535. Specify an asterisk (*) to display information for all records on the console. If the number of output lines exceeds the maximum number of lines for a multi-line WTO (Write to Operator) message, the report output is truncated.

This parameter applies to the ACCess, ALL, ALLConn, ARp, BYTEinfo, CACHinfo, COnn, DEFADDRT, DEvlinks, HOme, IDS, ND, PORTList, RESCache, ROUTe, SOCKets, SRCIP, VCRT, VDPT, VIPADCFG, and VIPADyn reports. The following list shows the descriptions of variations in support for the parameter for specific reports:

- DEvlinks report - The parameter and the values in the *n* OF *m* RECORDS DISPLAYED output line apply only to network interfaces that are defined with DEVICE or INTERFACE profile statements. These parameters and values do not apply to the LAN group or to the OSA-Express network traffic analyzer information.
- HOme - The parameter and the values in the *n* OF *m* RECORDS DISPLAYED output line apply to the IP addresses that are displayed by the report.

If this parameter is specified, it overrides the MAXRECS parameter value on the GLOBALCONFIG profile statement. If this parameter is not specified, the number of records value used for the report is one of the following vlaues:

- The MAXRECS parameter value that is specified on the GLOBALCONFIG TCP/IP profile statement.
- If the MAXRECS parameter is not specified, the MAXRECS parameter default value of 100 records.

The number of records that are displayed and the total number of records that could have been displayed are listed at the end of the report in the following output line, where *n* is the number of records that are displayed and *m* is the total number of records that could be displayed.

n OF *m* RECORDS DISPLAYED

If the report output is truncated, the *n* value specifies the number of records for which all output lines are successfully displayed.

Examples

DISPLAY TCPIP,,NETSTAT,ACCESS,NETWORK report

Use the DISPLAY TCPIP,,NETSTAT,ACCESS,NETWORK[,*ipaddr*] command to display the current NETACCESS profile statement configuration and associated security product information. When you specify the optional *ipaddr* value, the report is limited to the single NETACCESS entry, if any, that is currently being used by the stack for the specified IP address.

Parameters:

ipaddr
A fully qualified IPv4 or IPv6 IP address. Wildcard IP address values are not supported. This value is used to display the NETACCESS profile statement entry that governs the specified *ipaddr* value.

Examples:
Not IPv6 enabled (SHORT format):

```
 NETWORK ACCESS INFORMATION
 INBOUND: YES  OUTBOUND: YES      CACHE: ALL
 NETWORK PREFIX  ADDRESS MASK     SAF NAME
 DEFAULTHOME     <NONE>           DEFLTHOM
   PRFNM: EZB.NETACCESS.MVS00111.TCPCS100.DEFLTHOM  SECLABEL: SYSMULTI
 DEFAULT         <NONE>           DEFLT
   PRFNM: EZB.NETACCESS.*.*.*                       SECLABEL: OUTSIDER
 10.0.0.0        255.0.0.0        SITENET
   PRFNM: EZB.NETACCESS.*.*.SITE*                   SECLABEL: INTERNAL
 10.240.90.0     255.255.255.224  PAYROLL
   PRFNM: EZB.NETACCESS.*.*.PAYROLL                 SECLABEL: CONFACCT
 10.240.90.32    255.255.255.224  SALES
   PRFNM: EZB.NETACCESS.*.*.SALES                   SECLABEL: <NONE>
 10.240.90.64    255.255.255.224  TRAINING
   PRFNM: <NONE>                                    SECLABEL: <NONE>
 10.240.68.0     255.255.255.0    TESTFLOR
   PRFNM: EZB.NETACCESS.MVS00111.*.TESTFLOR         SECLABEL: SITEEAST
 7 OF  7 RECORDS DISPLAYED
 END OF THE REPORT
```

IPv6 enabled or request for LONG format:

```
NETWORK ACCESS INFORMATION
INBOUND: YES  OUTBOUND: YES  CACHE: ALL
SAF NAME  NETWORK PREFIX AND PREFIX LENGTH
--------  ------------------------------
DEFLTHOM  DEFAULTHOME
  PRFNM: EZB.NETACCESS.MVS00111.TCPCS100.DEFLTHOM  SECLABEL: SYSMULTI
DEFLT     DEFAULT
  PRFNM: EZB.NETACCESS.*.*.*                       SECLABEL: OUTSIDER
SITENET   10.0.0.0/8
  PRFNM: EZB.NETACCESS.*.*.SITE*                   SECLABEL: INTERNAL
PAYROLL   10.240.90.0/27
  PRFNM: EZB.NETACCESS.*.*.PAYROLL*                SECLABEL: CONFACCT
SALES     10.240.90.32/27
  PRFNM: EZB.NETACCESS.*.*.SALES                   SECLABEL: <NONE>
TRAINING  10.240.90.64/27
  PRFNM: <NONE>                                    SECLABEL: <NONE>
TESTFLOR  10.240.68.0/24
  PRFNM: EZB.NETACCESS.MVS00111.*.TESTFLOR         SECLABEL: SITEEAST
SITENET6  2001:0DB8:1::/64
  PRFNM: EZB.NETACCESS.*.*.SITE*                   SECLABEL: INTERNAL
PAYROLL6  2001:0DB8:1:0:9:67:115:66/128
  PRFNM: EZB.NETACCESS.*.*.PAYROLL*                SECLABEL: CONFACCT
7 OF 7 RECORDS DISPLAYED
END OF THE REPORT
```

Report field descriptions:
For a SHORT format report

INBOUND
Indicates whether Network Access Control is active for socket commands associated with inbound processing (accept, bind, and all variants of receive).

Yes Indicates that INBOUND is in effect (the INBOUND parameter was defined in the NETACCESS profile statement).

No Indicates that INBOUND is not in effect (the NOINBOUND parameter was defined or is in effect by default in the NETACCESS profile statement).

OUTBOUND
Indicates whether Network Access Control is active for socket commands associated with outbound processing (connect and all variants of send).

Yes Indicates that OUTBOUND is in effect (the OUTBOUND parameter was defined or is in effect by default in the NETACCESS profile statement).

No Indicates that OUTBOUND is not in effect (the NOOUTBOUND parameter was defined in the NETACCESS profile statement).

CACHE
Indicates the level of caching that is in effect for the Network Access Control access checking.

ALL Indicates that when a SAF call is made to check a user's access to a security zone, the result is cached regardless of whether access is permitted or denied.

PERMIT
Indicates that when a SAF call is made to check a user's access to a security zone, the result is cached when access is permitted, but not when access is denied.

SAME Indicates that when a SAF call is made to check a user's access to a security zone, the result is cached when access is permitted, but not when access is denied. In addition, if the user associated with the socket changes or if the IP address being accessed changes from the previous packet received or sent over the socket, a new SAF call is made for a previously permitted security zone.

SAF NAME
The final qualifier of a security product resource name. The maximum length is eight characters.

PRFNM
The security product profile covering this network security zone resource name. If no profile name covers this resource name or the SERVAUTH resource class is not active, the value `NONE` is displayed.

SECLABEL
The security label configured for the security product profile. If none is configured or the SECLABEL resource class is not active, the value `NONE` is displayed.

NETWORK PREFIX AND ADDRESS MASK
Can be one of the following case:

- The IPv4 IP address configured on a NETACCESS statement entry. It is logically ANDed with the ADDRESS MASK value to create the network address for which access control is required.
- The DEFAULTHOME entry configured on a NETACCESS statement entry. This entry is used for all IP addresses local to this stack that are not covered by a specific entry. This entry does not have an ADDRESS MASK.
- The DEFAULT entry configured on a NETACCESS statement entry. This entry is used for all IP addresses that are not covered by any other entry. This entry does not have an ADDRESS MASK.

For a LONG format report

INBOUND
Indicates whether Network Access Control is active for socket commands associated with inbound processing (accept, bind, and all variants of receive).

Yes Indicates that INBOUND is in effect (the INBOUND parameter was defined in the NETACCESS profile statement),

No Indicates that INBOUND is not in effect (the NOINBOUND parameter was defined or is in effect by default in the NETACCESS profile statement).

OUTBOUND
Indicates whether Network Access Control is active for socket commands associated with outbound processing (connect and all variants of send).

Yes Indicates that OUTBOUND is in effect (the OUTBOUND parameter was defined or is in effect by default in the NETACCESS profile statement).

No Indicates that OUTBOUND is not in effect (the NOOUTBOUND parameter was defined in the NETACCESS profile statement).

CACHE
Indicates the level of caching that is in effect for the Network Access Control access checking.

ALL Indicates that when a SAF call is made to check a user's access to a security zone, the result is cached regardless of whether access is permitted or denied.

PERMIT
Indicates that when a SAF call is made to check a user's access to a security zone, the result is cached when access is permitted, but not when access is denied.

SAME Indicates that when a SAF call is made to check a user's access to a security zone, the result is cached when access is permitted, but not when access is denied. In addition, if the user associated with the socket changes or if the IP address being accessed changes from the previous packet received or sent over the socket, a new SAF call is made for a previously permitted security zone.

SAF NAME
The final qualifier of a security product resource name. The maximum length is eight characters.

NETWORK PREFIX AND PREFIX LENGTH
Can be one of the following case:

- The IPv4 or IPv6 IP address and prefix length configured on a NETACCESS statement entry. (If an IPv4 network mask was configured, the prefix length is derived from it.) The prefix length specifies the left-most number of bits of the IP address to use to create the network address for which access control is required.
- The DEFAULTHOME entry configured on a NETACCESS statement entry. This entry is used for all IP addresses local to this stack that are not covered by a specific entry. This entry does not have a PREFIX LENGTH.
- The DEFAULT entry configured on a NETACCESS statement entry. This entry is used for all IP addresses that are not covered by any other entry. This entry does not have a PREFIX LENGTH.

PRFNM
The security product profile covering this network security zone resource name. If no profile name covers this resource name or the SERVAUTH resource class is not active, the value `NONE` is displayed.

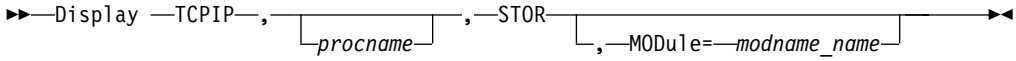
SECLABEL
The security label configured for the security product profile. If none is configured or the SECLABEL resource class is not active, the value `NONE` is displayed.

DISPLAY TCPIP,,STOR

Use the DISPLAY TCPIP,*procname*,STOR command to display TCP/IP storage usage information. You can use this command to verify the load module service level.

To verify load module service level, ensure that the eyecatcher for the module matches the latest PTF service for the module. When you contact IBM Service, you can use this command to verify that you are running on the correct TCP/IP service level.

Format



Parameters

STOR
Requests storage information.

If no other option is specified, the command displays the current and maximum storage usage for the TCP/IP stack and any TCP/IP storage limits. The maximum storage usage is the highest amount of storage TCP/IP has used since it started. See “Example” on page 240 for an example output, and see message EZZ8453I in z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM) for a description of the output displayed.

MODULE
Displays the load module name that contains the module, module address and the first 48 bytes of storage.

This command displays modules within load modules EZBTIINI, EZBITCOM, EZBPFINI, EZBTLMST, EZBTLCMN, and EZBTLCLG. This command does not provide information for the FTP TCP/IP modules.

Load module
Storage Location

EZBTIINI
Common storage

EZBITCOM
Common storage

EZBPFINI
OMVS private storage

EZBTLMST
TCP/IP private storage

EZBTLCMN
TCP/IP private storage

EZBTLCLG
TCP/IP private storage

Example

To display TCP/IP storage usage, issue the following command:

```
d tcpip,tcpip2,stor
EZZ8453I TCPIP STORAGE
EZZ8454I TCPIP2   STORAGE            CURRENT   MAXIMUM     LIMIT
EZD2018I 31-BIT
EZZ8455I          ECSA                45654K    56823K   204800K
EZZ8455I          PRIVATE            124634K   143743K   524288K
EZZ8455I          ECSA MODULES         8702K     8702K   NOLIMIT
EZD2018I 64-BIT
EZZ8455I          HVCOMMON               3M        3M   NOLIMIT
EZZ8455I          HVPRIVATE             50M       50M   NOLIMIT
EZZ8455I          TRACE HVCOMMON      2578M     2578M     2578M
EZZ8455I          SMC-R FIXEDMEMORY     12M       16M       40M
EZD2024I            SMC-R SEND MEMORY    4M        4M
EZD2024I            SMC-R RECV MEMORY    8M       12M
EZZ8455I          SMC-D FIXEDMEMORY     12M       16M       40M
EZZ8459I DISPLAY TCPIP STOR COMPLETED SUCCESSFULLY
```

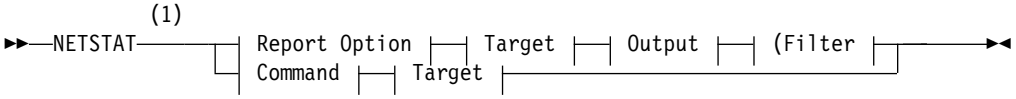
Usage

- If a module is built into multiple load modules, each occurrence is displayed.
- The storage display command is used to verify the load module service level of the TCP/IP stack. The command supports several, but not all, modules within the product.
- SMC-R memory information (messages EZZ8455I and EZD2024I) is included only when the Shared Memory Communications over Remote Direct Memory Access (SMC-R) function is or was enabled on this TCP/IP stack. The SMC-R function is enabled by using the SMCR parameter of the GLOBALCONFIG statement.
- SMC-D memory information (messages EZZ8455I) is included only when the Shared Memory Communications - Direct Memory Access (SMC-D) function is or was enabled on this TCP/IP stack. The SMC-D function is enabled by using the SMCD parameter of the GLOBALCONFIG statement.

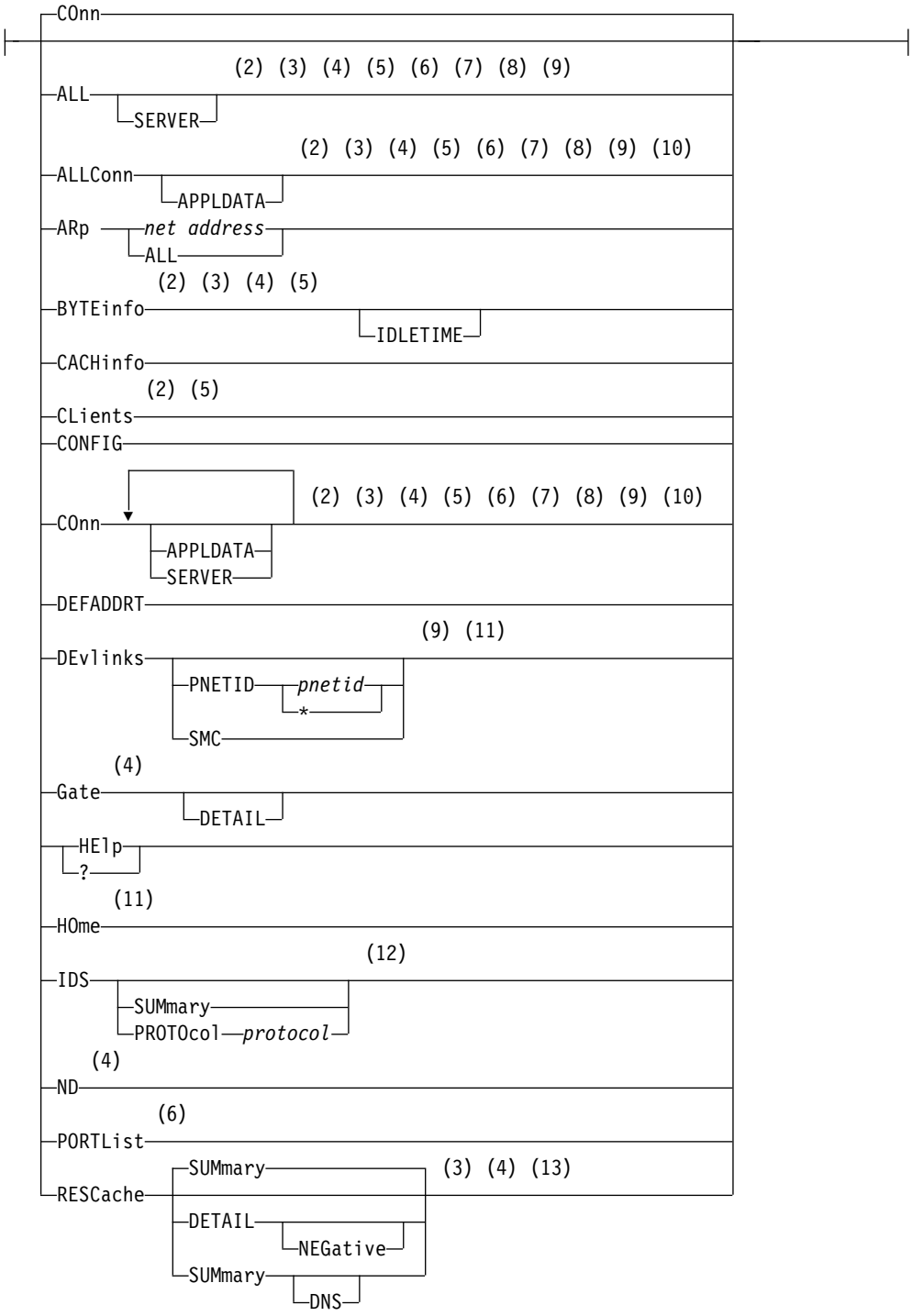
The TSO NETSTAT command syntax

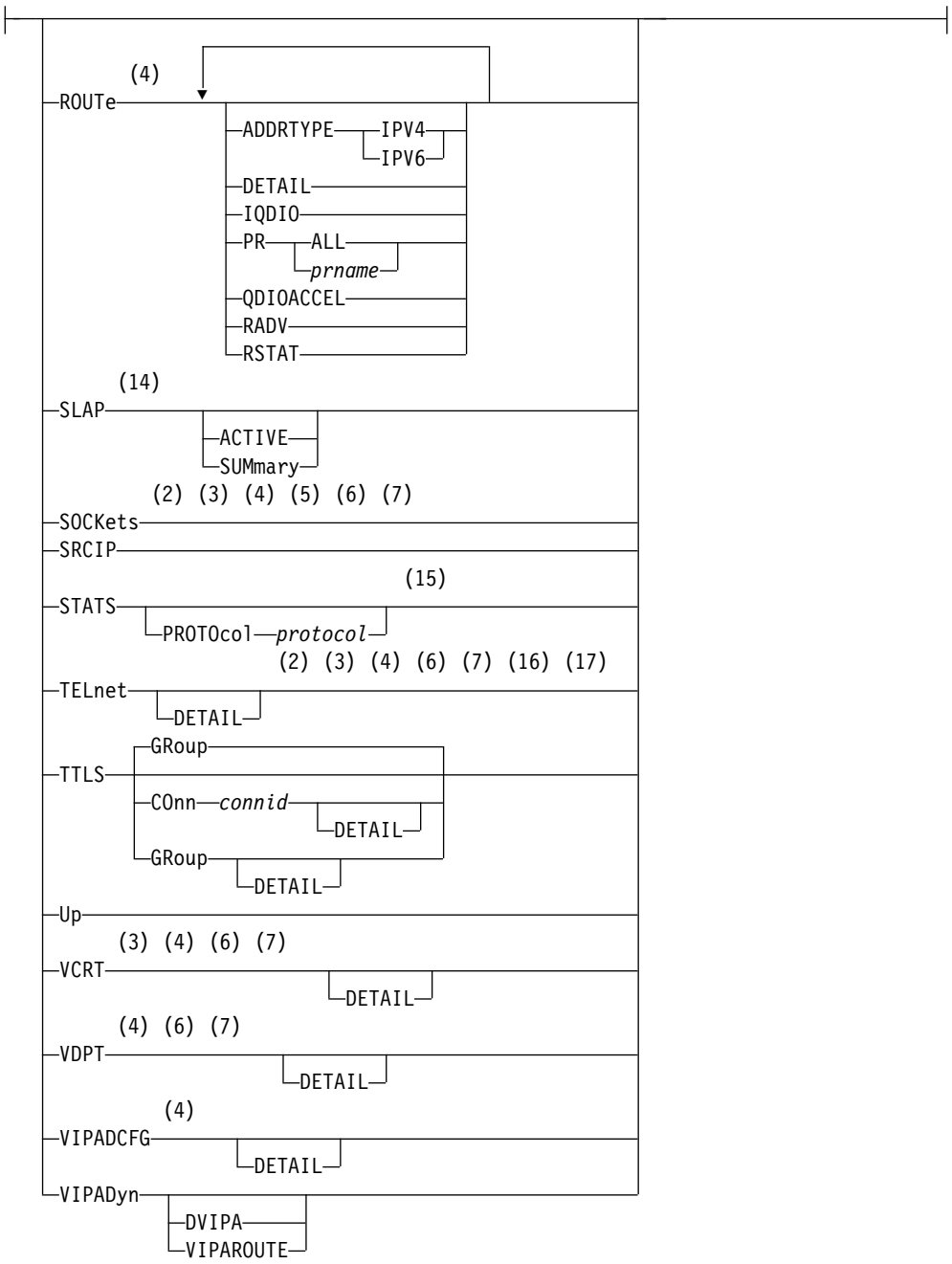
Use the TSO NETSTAT command to display the configuration and network status on a local TCP/IP stack.

Syntax

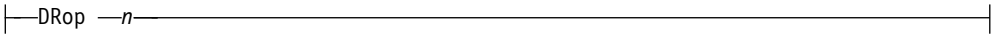


Report Option:


COnn
(2) (3) (4) (5) (6) (7) (8) (9)
ALL
SERVER
(2) (3) (4) (5) (6) (7) (8) (9) (10)
ALLConn
APPLDATA
ARp
net address
ALL
(2) (3) (4) (5)
BYTEinfo
IDLETIME
CACHinfo
(2) (5)
CLients
CONFIG
(2) (3) (4) (5) (6) (7) (8) (9) (10)
COnn
APPLDATA
SERVER
DEFADDRT
(9) (11)
DEvlinks
PNETID
pnetid
*
SMC
(4)
Gate
DETAIL
HElp
?
(11)
HOme
(12)
IDS
SUMmary
PROTOcol
protocol
(4)
ND
(6)
PORTList
(3) (4) (13)
RESCache
SUMmary
DETAIL
NEGative
SUMmary
DNS

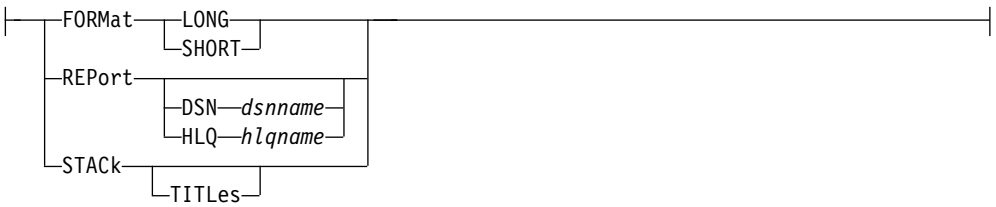


Command:

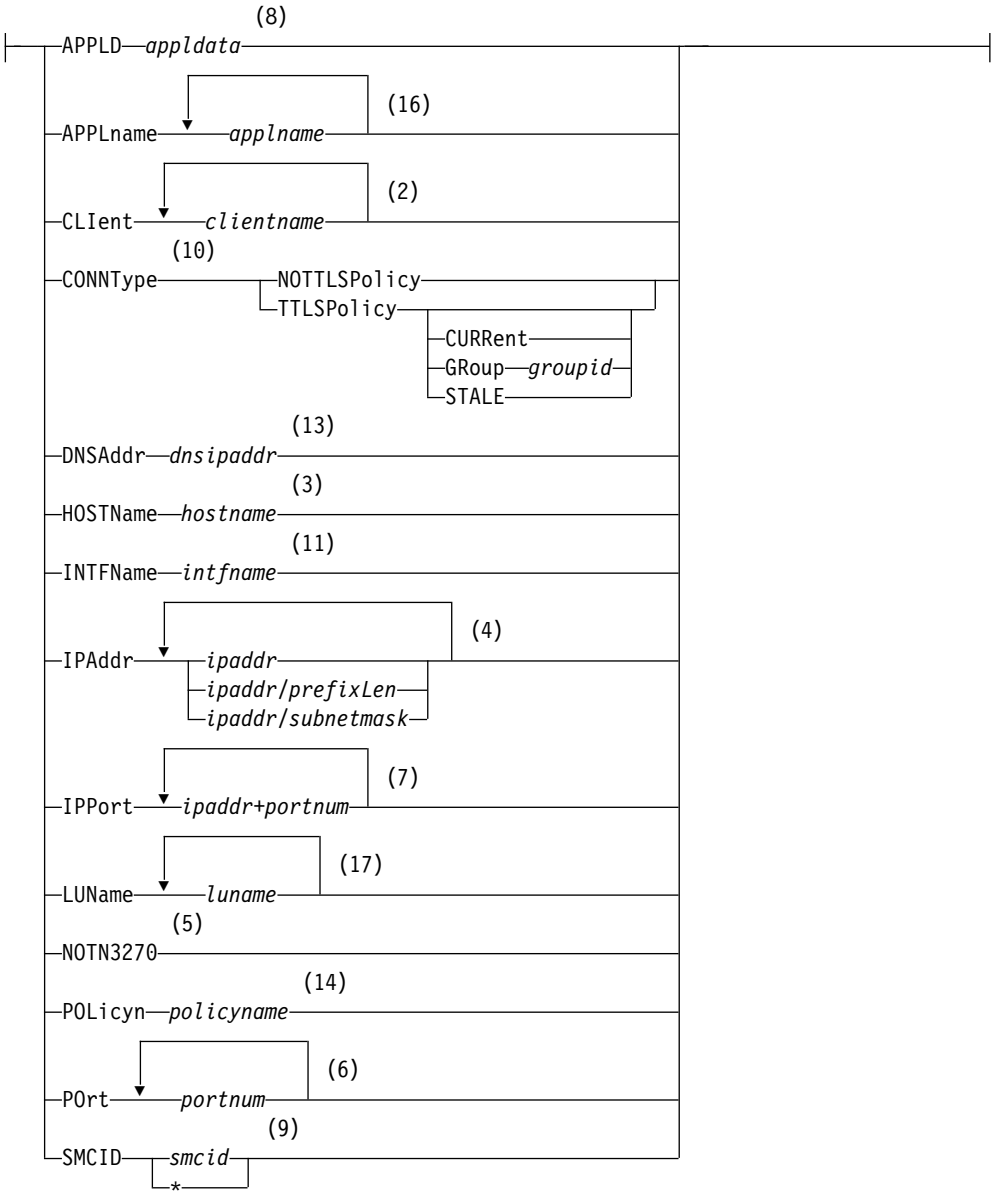


Target:

Output:



Filter:



Notes:

1 The minimum abbreviation for each parameter is shown in uppercase letters.

2 The CLIent filter is valid with ALL, ALLConn, BYTEinfo, COnn, CLients, SOCKets, and TELnet.

3 The HOSTName filter is valid only with ALL, ALLConn, BYTEinfo, COnn, RESCache, SOCKets, TELnet, and VCRT.

4 The IPAddr filter is valid only with ALL, ALLConn, BYTEinfo, COnn, Gate, ND, RESCache, ROUTe, SOCKets, TELnet, VCRT, and VDPT, and VIPADCFG.

5 The NOTN3270 filter is valid only with ALL, ALLConn, BYTEinfo, COnn, CLients, and SOCKets.

6 The POrt filter is valid only with ALL, ALLConn, COnn, PORTList, SOCKets, TELnet, VCRT, and VDPT.

7 The IPPort filter is valid only with ALL, ALLConn, COnn, SOCKets, TELnet, VCRT, and VDPT.

8 The APPLD filter is valid only with ALL, ALLConn, and COnn.

9 The SMCID filter is valid only with ALL, ALLConn, COnn, and DEvlinks.

10 The CONNType filter is valid only with ALLConn and COnn.

11 The INTFName filter is valid only with DEvlinks and HOme.

12 The valid protocol values are TCP and UDP.

13 The DNSAddr filter is valid only with RESCache.

14 The POLicyn filter is valid only with SLAP.

15 The valid protocol values are IP, ICMP, TCP, and UDP.

16 The APPLname filter is valid only with TELnet.

17 The LUName filter is valid only with TELnet.

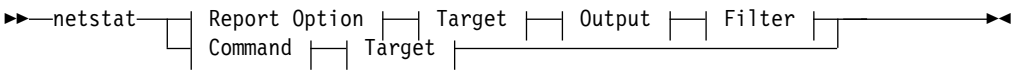
The z/OS UNIX netstat command syntax

Use the z/OS UNIX **netstat** command to display the network configuration and status on a local TCP/IP stack.

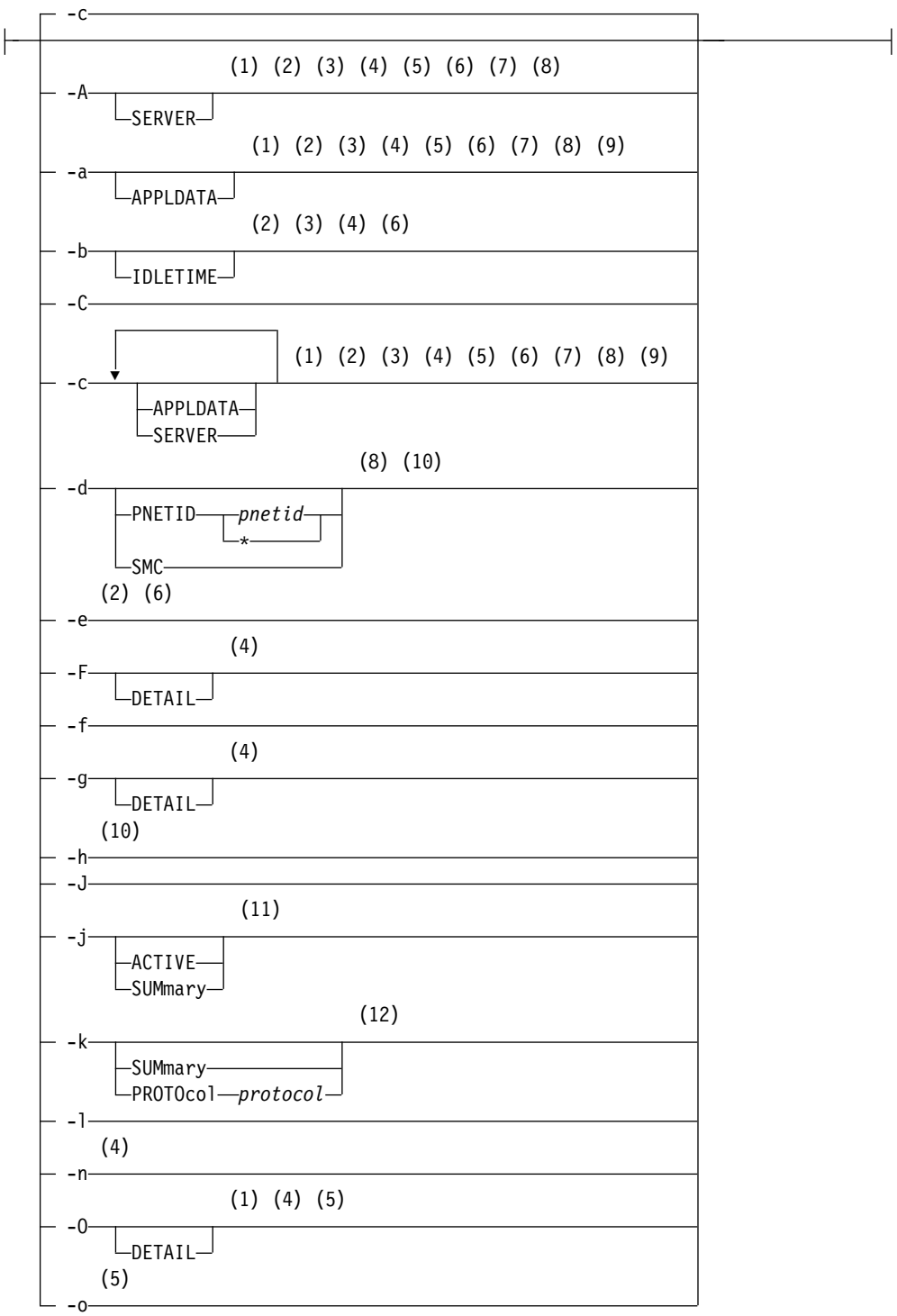
Note:

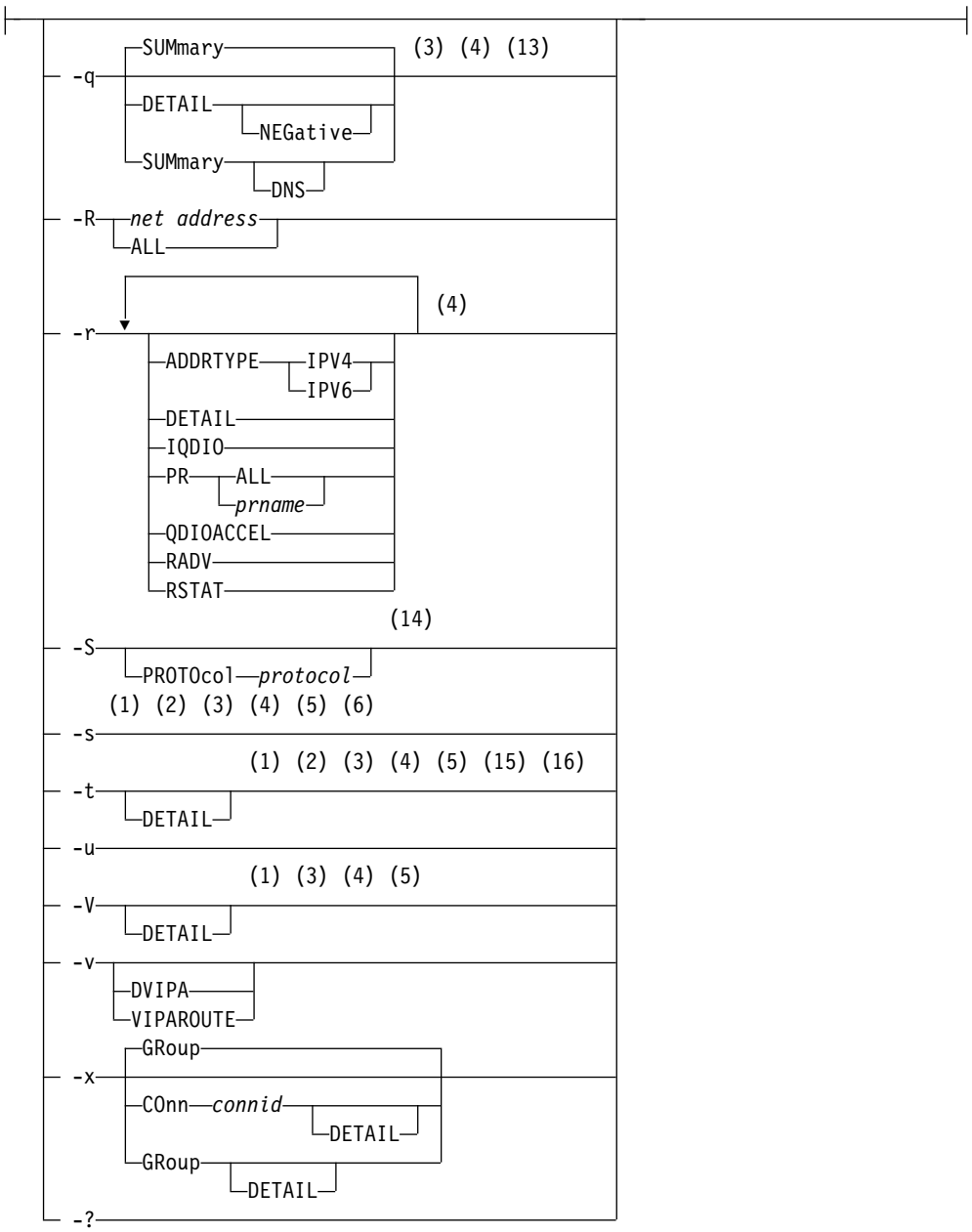
1. **netstat** is a synonym for the **onetstat** command in the z/OS UNIX shell. The **onetstat** command syntax is the same as that for the **netstat** command.
2. Some option modifiers for the z/OS UNIX **netstat** command are shown below using uppercase letters followed by lowercase letters (for example, SUMmary). The portion of the modifier shown using uppercase letters indicates the minimum abbreviation for the modifier. The modifier used must be entered using all uppercase letters.

Syntax



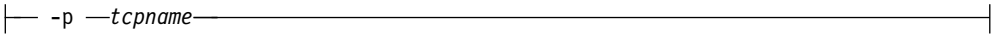
Report Option:


-c
(1) (2) (3) (4) (5) (6) (7) (8)
-A
SERVER
(1) (2) (3) (4) (5) (6) (7) (8) (9)
-a
APPLDATA
(2) (3) (4) (6)
-b
IDLETIME
-C
(1) (2) (3) (4) (5) (6) (7) (8) (9)
-c
APPLDATA
SERVER
(8) (10)
-d
PNETID
pnetid
*
SMC
(2) (6)
-e
(4)
-F
DETAIL
-f
(4)
-g
DETAIL
(10)
-h
-J
(11)
-j
ACTIVE
SUMmary
(12)
-k
SUMmary
PROTOcol
protocol
-l
(4)
-n
(1) (4) (5)
-O
DETAIL
(5)
-o



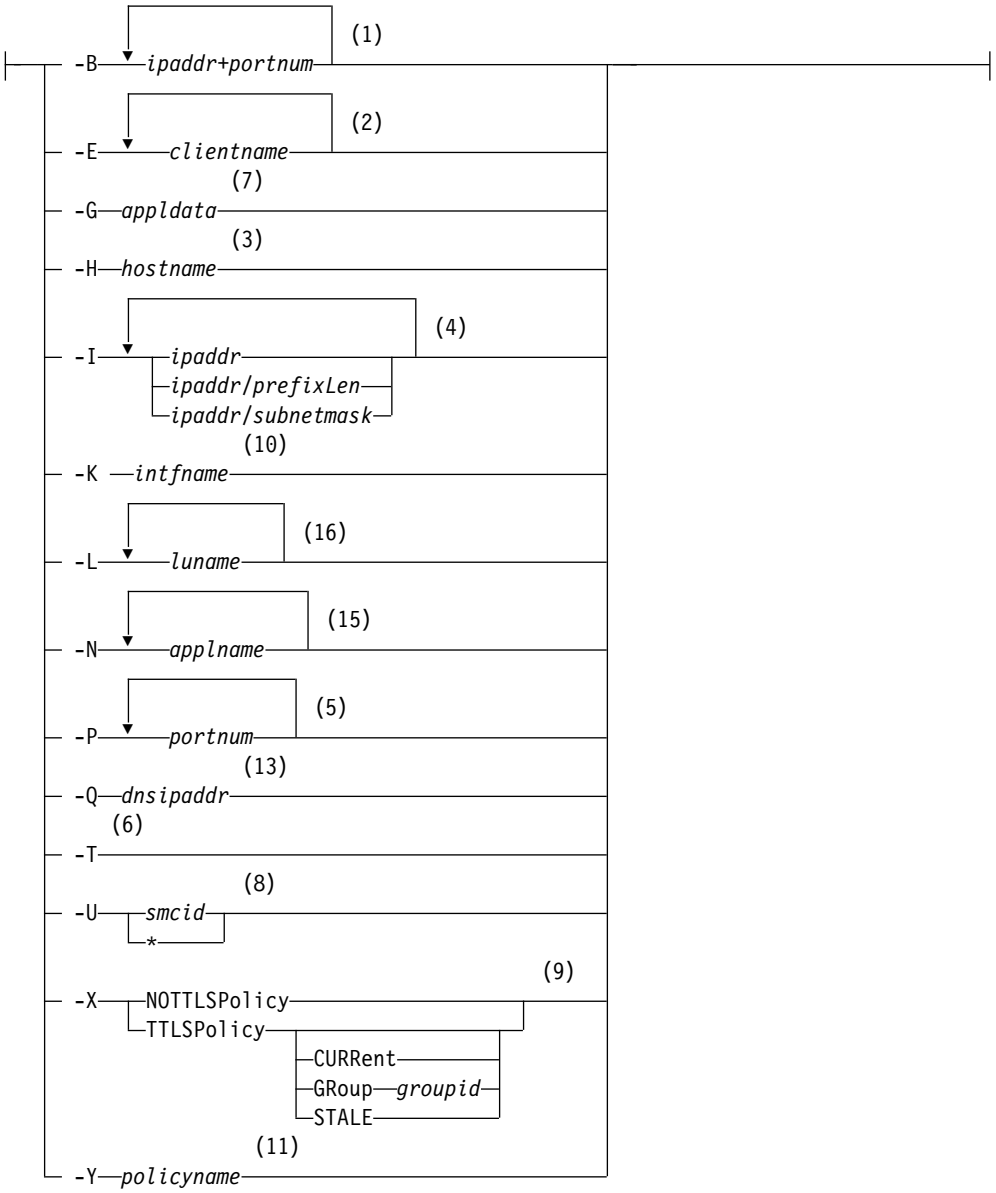
Command:

Target:



Output:

Filter:



Notes:

1 -B filter is valid only with -A, -a, -c, -s, -t, -O, and -V.

2 -E filter is valid only with -A, -a, -b, -c, -e, -s, and -t.

3 -H filter is valid only with -A, -a, -b, -c, -q, -s, -t, and -V.

4 -I filter is valid only with -A, -a, -b, -c, -F, -g, -n, -O, -q, -r, -s, -t, and -V.

5 -P filter is valid only with -A, -a, -c, -O, -o, -s, -t, and -V.

6 -T filter is valid only with -A, -a, -b, -c, -e, and -s.

7 -G filter is valid only with -A, -a, and -c.

8 -U filter is valid only with -A, -a, -c and -d.

9 -X filter is valid only with -a, and -c.

10 -K filter is valid only with -d and -h.

11 -Y filter is valid only with -j.

12 The valid protocol values are TCP, and UDP.

13 -Q filter is valid only with -q.

14 The valid protocol values are ICMP, IP, TCP, and UDP.

15 -N filter is valid only with -t.

16 -L filter is valid only with -t.

The Netstat command filter

The following parameters can be used to filter the output of the specified report. If you specify a filter parameter on the TSO NETSTAT command, it must be the last parameter on the command line preceded by a left parenthesis.

APPLD/-G *appldata*
Filter the output of the ALL/**-A**, ALLConn/**-a**, and COnn/**-c** reports using the specified application data *appldata*. You can enter one filter value at a time that can be 40 characters in length.

APPLname/-N *applname*
Filter the output of the TELnet/**-t** report using the specified VTAM application name *applname*. You can enter up to six filter values and each specified value can be eight characters in length.

CLIent/-E *clientname*
Filter the output of the ALL/**-A**, ALLConn/**-a**, BYTEinfo/**-b**, CLient/**-e**, COnn/**-c**, SOCKets/**-s**, and TELnet/**-t** reports using the specified client name *clientname*. You can enter up to six filter values and each specified value can be eight characters in length.

CONNType/-X
Filter the report using the specified connection type. You can enter one filter value at a time.

NOTTLSPolicy
Filter the output of the ALLConn/**-a** and COnn/**-c** reports, displaying only connections that have not been matched to an Application Transparent Transport Layer Security (AT-TLS) rule. This includes connections that were established while the AT-TLS function was disabled (the value NOTTLS was specified on the TCPCONFIG statement or is in effect by default) and all connections that are not TCP protocol. For TCP connections that were established when the AT-TLS function was enabled, this includes the following connections:

- Connections for which AT-TLS policy lookup has not yet occurred (typically the first send or receive has not yet been issued)
- Connections for which AT-TLS policy lookup has occurred but no matching rule was found

TTLSPolicy
Filter the output of the ALLConn/**-a** and COnn/**-c** reports, displaying only connections that match an Application Transparent Transport Layer Security (AT-TLS) rule. This includes only connections that were established while the AT-TLS function was

enabled, for which an AT-TLS policy rule was found with the value `TTLSEnabled ON` or `TTLSEnabled OFF` specified in the TTLSGroupAction. Responses can be further limited on AT-TLS connection type. AT-TLS connection type has the following values:

CURRent
Display only connections that are using AT-TLS where the rule and all actions are still available to be used for new connections.

GRoup *groupid*
Display only connections that are using the AT-TLSgroup specified by the *groupid* value. The specified *groupid* value is a number that is assigned by the TCP/IP stack to uniquely identify an AT-TLS group. You can determine the *groupid* value from the GroupID field that is displayed in the Netstat TTLS/**-x** GROUP report.

STALE
Display only connections that are using AT-TLS where the rule or at least one action is no longer available to be used for new connections.

DNSAddr/-Q *dnsaddr*
Filter the output of the RESCache/**-q** report using the specified DNS IP address *dnsaddr*. You can enter one filter value at a time. The specified IPv4 *dnsaddr* value can be 1–15 characters in length; the specified IPv6 *dnsaddr* value can be 1–45 characters in length.

Restriction: The DNSAddr/**-Q** filter does not support wildcard characters.

HOSTName/-H *hostname*
Filter the output of the ALL/**-A**, ALLConn/**-a**, BYTEinfo/**-b**, COnn/**-c**, RESCache/**-q**, SOCKets/**-s**, TELnet/**-t**, and VCRT/**-V** reports using the specified host name value *hostname*. You can enter one filter value at a time and the specified value can be up to 255 characters in length.

Result: For reports other than those produced using the RESCache/**-q** option, at the end of the report, the Netstat command displays the host name that the resolver used for the resolution and the list of IP addresses returned from the resolver that it used as filters.

Restrictions:

1. The HOSTName/**-H** filter supports wildcard characters only for the RESCache/**-q** option, but not for other options.
2. With options other than the RESCache/**-q** option, using the HOSTName filter might cause delays in the output because the *hostname* value must be resolved (depending on resolver and DNS configuration).
3. For the RESCache/**-q** option, the HOSTName/**-H** filter applies only to the HostName to IPAddress translation portion of the report.

INTFName/-K *intfname*
Filter the output of the DEvlinks/**-d** and HOme/**-h** reports using the specified interface name value *intfname*. You can enter one filter value at a time and the specified value can be 1–16 characters in length.

For the DEvlinks and HOme report options, the INTFName filter can be one of the following names:

- The network interface name that was displayed in the LnkName/LinkName or INTFName field in the report (this option selects one interface).
- The port name of an OSA-Express feature in QDIO mode. This is the name that is specified on the PORTNAME keyword in the TRLE (this option selects all interfaces that are associated with the OSA-Express port, including an OSAENTA trace interface).
- The name of a HiperSockets TRLE (this option selects all interfaces that are associated with the HiperSockets TRLE).

Additionally, for the DEvlinks report option, the INTFName filter can also be the interface name of an OSAENTA trace interface, which is EZANTA*portname*, where the *portname* value is the name that is specified on the PORTNAME keyword in the TRLE for the OSA-Express port that is being traced (this option selects one interface). The INTFName/-K filter is not supported for the DEvlinks/-d report if the PNETID modifier is specified.

Guideline: For the DEvlinks/**-d** option, if a network resource has been coded in TCPIP.PROFILE using the DEVICE/LINK/HOME statements, then the *intfname* value that should be used is the link name that was specified on the LINK profile statement. Otherwise, use the interface name that was specified on the INTERFACE profile statement.

Restriction: The INTFName filter does not support wildcard characters.

IPAddr/-I *ipaddr***IPAddr/-I** *ipaddr/prefixlength***IPAddr/-I** *ipaddr/subnetmask*
Filter the report output using the specified IP address *ipaddr*, *ipaddr/prefixlength*, or *ipaddr/subnetmask*. For options other than the RESCache/**-q** option, you can enter up to six filter values; the RECache**/-q** option accepts only one filter value at a time in *ipaddr* format. Each specified IPv4 *ipaddr* value can be 1–15 characters in length and each selected IPv6 *ipaddr* value can be 1–45 characters in length.

ipaddr Filter the output of the ALL/**-A**, ALLConn/**-a**, BYTEinfo/**-b**, COnn/**-c**, Gate/**-g**, ND/**-n**, RESCache/**-q**, ROUTe/**-r**, SOCKets/**-s**, TELnet/**-t**, VCRT/**-V**, VDPT/**-O**, and VIPADCFG/**-F** reports using the specified IP address *ipaddr*. For all options except the RESCache/**-q** option, the default subnet mask 255.255.255.255 is used for IPv4 addresses; for IPv6 addresses, the default *prefixlength* value 128 is used. The RECache/**-q** option does not support any default subnet mask or default *prefixlength* values.

ipaddr/prefixlength
Filter the output of the ALL/**-A**, ALLConn/**-a**, BYTEinfo/**-b**, COnn/**-c**, ND/**-n**, ROUTe/**-r**, SOCKets/**-s**, TELnet/**-t**, VCRT/**-V**, VDPT/**-O**, and VIPADCFG/**-F** reports using the specified IP address and prefix length *ipaddr/prefixlength*. For an IPv4 address, the prefix length range is 1 – 32. For an IPv6 address, the prefix length range is 1 – 128.

ipaddr/subnetmask
Filter the output of the ALL/**-A**, ALLConn/**-a**, BYTEinfo/**-b**, COnn/**-c**, Gate/**-g**, ROUTe/**-r**, SOCKets/**-s**, TELnet/**-t**, VCRT/**-V**, VDPT/**-O**, and VIPADCFG/**-F** reports using the specified IP address and subnet mask *ipaddr/subnetmask*. The IP address *ipaddr* in this format must be an IPv4 IP address.

Note:

1. For the Gate/**-g** option, *ipaddr* is the destination IP address; it is not the destination network address.
2. When filtering Gate/**-g** and ROUTe/**-r** outputs on a specified IP address, the DEFAULT and DEFAULTNET routes are not displayed.

Guidelines:

- For ALL/**-A**, ALLConn/**-a**, COnn/**-c**, and TELnet/**-t** options, *ipaddr* can be either the local or remote IP address. For the BYTEinfo/**-b** option, *ipaddr* can be a remote IP address. For the SOCKets/**-s** option, *ipaddr* can be an address to which the socket is bound or connected. For the VCRT/**-V** option, *ipaddr* can be a source IP address, a destination IP address, or a destination XCF IP address. For the VDPT/**-O** option, *ipaddr* can be a destination IP address or a destination XCF IP address. For the VIPADCFG/**-F** option, *ipaddr* can be a dynamic VIPA address, a destination IP address, or a destination XCF IP address.
- For an IPv6-enabled stack (except for RESCache/**-q** option):
  - Both IPv4 and IPv6, *ipaddr* values are accepted and can be mixed on the IPAddr/**-I** option.
  - For an IPv6-enabled stack, an IPv4-mapped IPv6 address is accepted as a valid *ipaddr* value and usually provides the same result as its IPv4 address. But, for ROUTE/**-r** and ND/**-n** options, an IPv4-mapped IPv6 address is treated as an IPv6 address. If an IPv4-mapped IPv6 address is entered as an *ipaddr* value for these two options, no matching entry is found.
- For the RESCache/**-q** option, the *ipaddr* value can be either an IPv4 or IPv6 address regardless of whether the stack is configured for IPv4 or IPv6 operation.

Restrictions:

- The IPAddr/**-I** filter for RESCache/**-q**, VCRT/**-V**, VDPT/**-O**, and VIPADCFG/**-F** options does not support wildcard characters.
- The IPAddr/**-I** filter for an IPv6 address does not support wildcard characters.
- For a UDP endpoint socket, the filter value applies only to the local or source IP address.
- For all options except the RESCache/**-q** option, for an IPv4-only stack, only IPv4 *ipaddr* values are accepted. The RECache/**-q** option always accepts IPv4 and IPv6 addresses, regardless of the capability of the stack.
- For the ND/**-n** option, an IPv4 *ipaddr* value is not accepted.
- For the RESCache/**-q** option, the IPAddr/-I filter applies only to the IPAddress to HostName translation portion of the report.
- The RECache/**-q** option accepts only one filter value at a time in *ipaddr* format.

IPPort/-B *ipaddr+portnum*

Filter the report output of the ALL/**-A**, ALLConn/**-a**, CONN/**-c**, SOCKets/**-s**, TELnet/**-t**, VCRT/**-V**, and VDPT/**-O** reports using the specified IP address and port number. You can enter up to six filter values. Each specified IPv4 *ipaddr* value can be up to 15 characters in length, denoting a single IPv4 IP address; each specified IPv6 *ipaddr* value can be up to 45 characters in length, denoting a single IPv6 IP address. Valid

portnum values are in the range 0 – 65535. The filter values *ipaddr* and *portnum* will match any combination of the local and remote IP address and local and remote port.

Guidelines:

- For the ALL/**-A**, ALLConn/**-a**, COnn/**-c**, and TELnet/**-t** options, the *ipaddr* value can be either the local or remote IP address. For the SOCKets/**-s** option, the *ipaddr* value can be an address to which the socket is bound or connected. For the VCRT/**-V** option, the *ipaddr* value can be a source IP address, a destination IP address, or a destination XCF IP address. For the VDPT/**-O** option, the *ipaddr* value can be a destination IP address or a destination XCF IP address.
- For an IPv6-enabled stack, the following apply:
  - Both IPv4 and IPv6 *ipaddr* values are accepted and can be mixed on the IPPort/**-B** option.
  - An IPv4-mapped IPv6 address is accepted as a valid *ipaddr* value and usually provides the same result as the IPv4 address.

Restrictions:

- The *ipaddr* value in the IPPort/**-B** filter does not support wildcard characters.
- For an IPv4-only stack, only IPv4 *ipaddr* values are accepted.
- For a UDP endpoint socket, the filter value applies only to the local or source IP address and port.
- An entry is returned only when both the *ipaddr* and *portnum* values match.

LUName/-L *luname*
Filter the output of the TELnet/**-t** report using the specified LU name *luname*. You can enter up to six filter values and each specified value can be up to eight characters in length.

NOTN3270/-T
Filter the output of the ALL/**-A**, ALLConn/**-A**, BYTEinfo/**-b**, CLient/**-e**, COnn/**-c**, and SOCKets/**-s** reports, excluding TN3270 server connections.

POLicyn/-Y *policyname*
Filter the output of the SLAP/**-j** report using the specified policy rule name *policyname*. You can enter one filter value at a time and the specified value can be up to 48 characters in length.

POrt/-P *portnum*
Filter the output of the ALL/**-A**, ALLConn/**-a**, COnn/**-c**, PORTList/**-o**, SOCKets/**-s**, TELnet/**-t**, VCRT/**-V**, and VDPT/**-O** reports using the specified port number *portnum*. You can enter up to six filter values.

Guidelines:

- The port number can be either a local port or a remote port.

  For the SOCKets/**-s** option, the port can be a port to which the socket is bound or connected.
- For the ALL/**-A**, ALLConn/**-a**, COnn/**-c**, SOCKets/**-s**, TELnet/**-t**, VCRT/**-V**, and VDPT/**-O** reports, the port value range is 0-65535
- For the PORTList/**-o** option only, the port value range is 1-65535 and you can also filter on the keyword UNRSV

Restriction:

- No wildcards are allowed.
- For a UDP endpoint socket, the filter value applies only to the local or source IP address.

SMCID/-U *smcid*
Filter the output of the ALL/-A, ALLConn/-a, COnn/-c, and DEvlinks/-d reports by using the specified Shared Memory Communications over Remote Direct Memory Access (SMC-R) link, SMC-R link group, or Shared Memory Communications - Direct Memory Access (SMC-D) link identifier *smcid*. If an asterisk (*) is specified for the filter value, Netstat provides output only for the entries that are associated with SMC-R links, SMC-R link groups, and SMC-D links. You can enter one filter value at a time. The SMCID filter is not supported for the DEvlinks/-d report if the PNETID modifier is specified.

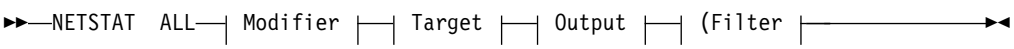
Except for POrt/**-P**, INTFName/**-K**, CONNType/**-X** TTLSPolicy GRoup *groupid*, DNSAddr/**-Q**, SMCID/**-U** and IPPort/**-B**, the filter value can be a complete or partial string using wildcard characters. A wildcard character can be an asterisk (*), which matches a null string or any character or character string, at the same position. A wildcard character can be a question mark (?), which matches any single character at the same position. For example, a string *searchee* matches with **ar?he**, but the string *searhee* does not match with **ar?he**. If you want to use the wildcard character on the IPAddr/**-I** parameter, you must specify the value in the *ipaddr* format. The wildcard character is not accepted for the *ipaddr/subnetmask* or *ipaddr/prefixlen* format of IPAddr/**-I** values.

When you use z/OS UNIX **netstat**/**onetstat** command in a z/OS UNIX shell environment, take care when you use a z/OS UNIX MVS special character in a character string such as using a wildcard character in a filter value. It might cause an unpredictable result. To be safe, if you want to use a z/OS UNIX MVS special character in a character string, surround the character string with single (') or double (") quotation marks. For example, to use an asterisk (*) in the IP address, 10.*.0.0 for the **-I** filter, issue the command as: **netstat -g -I '10.*.0.0'** or **netstat -g -I "10.*.0.0"**.

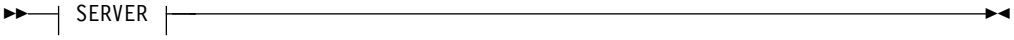
Netstat ALL/-A report

Displays detailed information about TCP connections and UDP sockets, including some recently closed ones. The purpose of this report is to aid in debugging problems with TCP connections and UDP sockets.

TSO syntax



Modifier



SERVER
Provide detailed information only for TCP connections that are in the listen state.

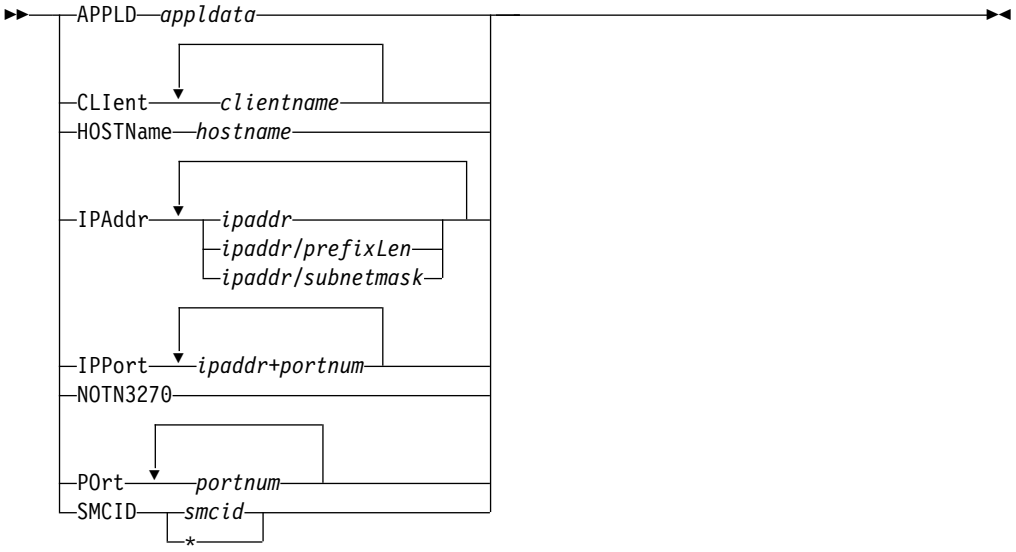
Target

Provide the report for a specific TCP/IP address space by using TCp *tcpname*. See The Netstat command target for more information about the TCp parameter.

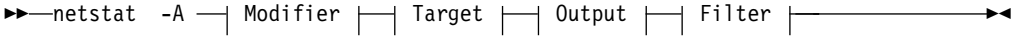
Output

The default output option displays the output on the user's terminal. For other options, see "The TSO NETSTAT command syntax" on page 241 or Netstat command output.

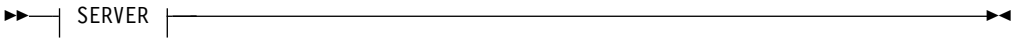
Filter



Netstat ALL/-A report z/OS UNIX syntax



Modifier



SERVER

Provide detailed information only for TCP connections that are in the listen state.

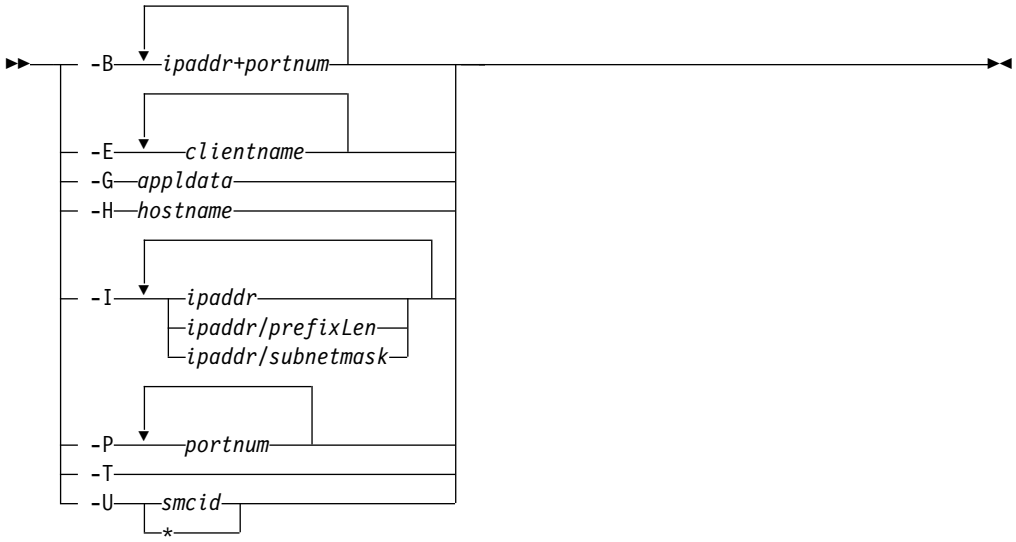
Target

Provide the report for a specific TCP/IP address space by using **-p** *tcpname*. See The Netstat command target for more information about the **-p** parameter.

Output

The default output option displays the output to z/OS UNIX shell stdout. For other options, see "The z/OS UNIX netstat command syntax" on page 245 or Netstat command output.

Filter



Filter description

APPLD/-G *appldata*
Filter the output of the ALL/**-A** report using the specified application data *appldata*. You can enter one filter value at a time and the specified value can be 40 characters in length.

CLIent/-E *clientname*
Filter the output of the ALL/**-A** report using the specified client name *clientname*. You can enter up to six filter values and each specified value can be eight characters in length.

HOSTName/-H *hostname*
Filter the output of the ALL/**-A** report using the specified host name *hostname*. You can enter one filter value at a time and the specified value can be up to 255 characters in length.

Result: At the end of the report, Netstat displays the host name that the resolver used for the resolution and the list of IP addresses returned from the resolver that it used as filters.

Restrictions:

1. The HOSTName/**-H** filter does not support wildcard characters.
2. Using the HOSTName/**-H** filter might cause delays in the output due to resolution of the *hostname* value depending upon resolver and DNS configuration.

IPAddr/-I *ipaddr***IPAddr/-I** *ipaddr/prefixlength***IPAddr/-I** *ipaddr/subnetmask*
Filter the report output using the specified IP address *ipaddr*, *ipaddr/prefixlength*, or *ipaddr/subnetmask*. You can enter up to six filter values. Each specified IPv4 *ipaddr* value can be up to 15 characters in length and each selected IPv6 *ipaddr* value can be 45 characters in length.

ipaddr Filter the output of the ALL/**-A** report using the specified IP address *ipaddr*. For IPv6 addresses, the default *prefixlength* 128 is used.

ipaddr/prefixlength
Filter the output of the ALL/**-A** report using a specified IP address and prefix length *ipaddr/prefixlength*. For an IPv4 address, the prefix length range is 1 – 32. For an IPv6 address, the prefix length range is 1 – 128.

ipaddr/subnetmask
Filter the output of the ALL/**-A** report using the specified IP address and subnet mask *ipaddr/subnetmask*. The IP address *ipaddr* in this format must be an IPv4 IP address.

Guidelines:

1. The filter value *ipaddr* can be either the local or remote IP address.
2. For an IPv6-enabled stack:
   - Both IPv4 and IPv6 *ipaddr* values are accepted and can be mixed on the IPAddr/**-I** option.
   - An IPv4-mapped IPv6 address is accepted as a valid *ipaddr* value and usually provides the same result as its IPv4 address.

Restrictions:

1. For an IPv4-only stack, only IPv4 *ipaddr* values are accepted.
2. The filter value for an IPv6 address does not support wildcard characters.
3. For a UDP endpoint socket, the filter value applies only to the local or source IP address.

IPPort/-B *ipaddr+portnum*
Filter the report output of the ALL/**-A** report using the specified IP address and port number. You can enter up to six filter values. Each specified IPv4 *ipaddr* value can be up to 15 characters in length, denoting a single IPv4 IP address; each specified IPv6 *ipaddr* value can be up to 45 characters in length, denoting a single IPv6 IP address. Valid *portnum* values are in the range 0 – 65535. The filter values *ipaddr* and *portnum* will match any combination of the local and remote IP address and local and remote port.

Guidelines:

- The filter value *ipaddr* can be either the local or remote IP address.
- For an IPv6-enabled stack, the following apply:
  – Both IPv4 and IPv6 *ipaddr* values are accepted and can be mixed on the IPPort/**-B** option.
  – An IPv4-mapped IPv6 address is accepted as a valid *ipaddr* value and usually provides the same result as the IPv4 address.

Restrictions:

- The *ipaddr* value in the IPPort/**-B** filter does not support wildcard characters.
- For an IPv4-only stack, only IPv4 *ipaddr* values are accepted.
- An entry is returned only when both the *ipaddr* and *portnum* values match.
- For a UDP endpoint socket, the filter value applies only to the local or source IP address and port.

NOTN3270/-T
Filter the output of the ALL/**-A** report, excluding TN3270 server connections.

POrt/-P *portnum*
Filter the output of the ALL/**-A** report using the specified port number *portnum*. You can enter up to six filter values. For all *portnum* values that were reserved by the same PORTRANGE profile statement, only one output line is displayed.

Guideline: The port number can be either a local or remote port.

Restriction: For a UDP endpoint socket, the filter value applies only to the local or source port.

SMCID/-U *smcid*
Filter the output of the ALL/-A report by using the specified Shared Memory Communications over Remote Direct Memory Access (SMC-R) link, SMC-R link group, or Shared Memory Communications - Direct Memory Access (SMC-D) link identifier *smcid*. If an asterisk (*) is specified for the filter value, Netstat provides output only for the entries that are associated with SMC-R links, SMC-R link groups, and SMC-D links. You can enter one filter value at a time.

The filter value for CLIent/**-E**, IPAddr/**-I**, and APPLD/-G can be a complete string or a partial string using wildcard characters. A wildcard character can be an asterisk (*), which matches a null string or any character or character string, at the same position. A wildcard character can be a question mark (?), which matches any single character at the same position. For example, a string *searchee* matches with **ar?he**, but the string *searhee* does not match **ar?he**. To use the wildcard character on the IPAddr/**-I** filter, specify the value in the *ipaddr* format. The wildcard character is not accepted for the *ipaddr/prefixlen* or *ipaddr/subnetmask* format of IPAddr/**-I** values.

When you use z/OS UNIX **netstat**/**onetstat** command in a z/OS UNIX shell environment, take care if you use a z/OS UNIX MVS special character in a character string. It might cause an unpredictable result. To be safe, if you want to use a z/OS UNIX MVS special character in a character string, surround the character string with single (') or double (") quotation marks. For example, to use an asterisk (*) in the IP address, 10.*.0.0 for the **-I** filter, issue the command as: **netstat -A -I '10.*.0.0'**.

Command syntax examples

From TSO environment

```
NETSTAT ALL
   Display detailed information about TCP connections and UDP sockets in the default
   TCP/IP stack.
NETSTAT ALL TCP TCPCS6
   Display detailed information about TCP connections and UDP sockets in TCPCS6 stack.
NETSTAT ALL TCP TCPCS8 (IPADDR 9.43.1.1 9.43.2.2
   Display detailed information about those TCP connections and UDP sockets in TCPCS8
   stack whose local or remote IP addresses match the specified filter IP address values.
NETSTAT ALL (PORT 2222 6666 88
   Display detailed information about those TCP connections and UDP sockets in the
   default TCP/IP stack whose local or remote ports match the specified filter port
   numbers.
NETSTAT ALL SERVER TCP TCPCS
   Display detailed information about those TCP connections in listen state on
   TCP/IP stack TCPCS
NETSTAT ALL TCP TCPCS (IPPORT 127.0.0.1+21
   Display detailed information about connections using ip address 127.0.0.1 and
   port 21 on TCP/IP stack TCPCS
```

From UNIX shell environment

```
   netstat -A
   netstat -A -p tcpcs6
   netstat -A -p tcpcs6 -I 9.43.1.1 9.43.2.2
   netstat -A -P 2222 6666 88
   netstat -A SERVER -p tcpcs
   netstat -A -B 127.0.0.1+21 -p tcpcs
```

Report examples

The following examples are generated by using TSO NETSTAT command. Using the z/OS UNIX **netstat** command displays the data in the same format as the TSO NETSTAT command.

Not IPv6 enabled (SHORT format)

```
NETSTAT ALL MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           22:24:30
Client Name: FTPD1                    Client Id: 000000F9
Local Socket: 9.42.104.43..21         Foreign Socket: 9.42.103.165..1035
  BytesIn:            0000000035        BytesOut:           0000000265
  SegmentsIn:         0000000017        SegmentsOut:        0000000014
  StartDate:          01/09/2012        StartTime:          22:04:11
  Last Touched:       22:04:18          State:              Establsh
  RcvNxt:             0214444666        SndNxt:             0216505563
  ClientRcvNxt:       0214443596        ClientSndNxt:       0216504670
  InitRcvSeqNum:      0214443560        InitSndSeqNum:      0216504404
  CongestionWindow:   0000007336        SlowStartThreshold: 0000065535
  IncomingWindowNum:  0214477396        OutgoingWindowNum:  0216538247
  SndWl1:             0214444666        SndWl2:             0216505563
  SndWnd:             0000032684        MaxSndWnd:          0000032768
  SndUna:             0216505563        rtt_seq:            0216505479
  MaximumSegmentSize: 0000000524        DSField:            00
  Round-trip information:
    Smooth trip time: 102.000           SmoothTripVariance: 286.000
  ReXmt:              0000000000        ReXmtCount:         0000000000
  DupACKs:            0000000000        RcvWnd:             0000032730
  SockOpt:            85                TcpTimer:           00
  TcpSig:             84                TcpSel:             60
  TcpDet:             E0                TcpPol:             00
  TcpPrf:             C0                TcpPrf2:            70
  TcpPrf3:            00
  DelayAck:           AutoYes
  QOSPolicy:          No
  TTLSPolicy:         Yes
    TTLSRule:         server
    TTLSGrpAction:    group_action1
    TTLSEnvAction:    Environment1
  RoutingPolicy:      No
  ReceiveBufferSize:  0000016384        SendBufferSize:     0000016384
  ReceiveDataQueued:  0000000000
  SendDataQueued:     0000000000
  SendStalled:        No
  Ancillary Input Queue: Yes
    BulkDataIntfName: OSAQDIO4
  Application Data:   EZAFTP0S C USER1     PTS305
----
```

```
Client Name: US16SVR                  Client Id: 0000000D
Local Socket: 0.0.0.0..10007          Foreign Socket: 0.0.0.0..0
  BytesIn:            0000024000        BytesOut:           0000032000
  SegmentsIn:         0000000900        SegmentsOut:        0000001000
  StartDate:          03/20/2014        StartTime:          17:53:16
  Last Touched:       17:53:16          State:              Listen
  RcvNxt:             0000000000        SndNxt:             0000000000
  ClientRcvNxt:       0000000000        ClientSndNxt:       0000000000
  InitRcvSeqNum:      0000000000        InitSndSeqNum:      0000000000
  CongestionWindow:   0000000000        SlowStartThreshold: 0000000000
  IncomingWindowNum:  0000000000        OutgoingWindowNum:  0000000000
  SndWl1:             0000000000        SndWl2:             0000000000
  SndWnd:             0000000000        MaxSndWnd:          0000000000
  SndUna:             0000000000        rtt_seq:            0000000000
  MaximumSegmentSize: 0000000536        DSField:            00
  Round-trip information:
    Smooth trip time: 0.000             SmoothTripVariance: 1500.000
  ReXmt:              0000000000        ReXmtCount:         0000000000
  DupACKs:            0000000000        RcvWnd:             0000131072
  SockOpt:            00                TcpTimer:           00
  TcpSig:             00                TcpSel:             20
  TcpDet:             C0                TcpPol:             00
  TcpPrf:             00
  QOSPolicy:          No
  RoutingPolicy:      No
  ReceiveBufferSize:  0000065536        SendBufferSize:     0000065536
  ConnectionsIn:      0000000010        ConnectionsDropped: 0000000000
  MaximumBacklog:     0000000004        ConnectionFlood:    No
  CurrentBacklog:     0000000000
    ServerBacklog:    0000000000        FRCABacklog:        0000000000
  CurrentConnections: 0000000005        SEF:                100
  Quiesced:           No
  SMC Information:
    SMCDCurrConns:    0000000002        SMCDTotalConns:     0000000015
    SMCRCurrConns:    0000000004        SMCRTotalConns:     0000000008
    UseSMC:           Yes               Source:             AutoSMC
    AutoSMC%:         090
----
```

```
Client Name: FTPD1                    Client Id: 000000F6
Local Socket: 0.0.0.0..21             Foreign Socket: 0.0.0.0..0
  BytesIn:            0000000000        BytesOut:           0000000000
  SegmentsIn:         0000000000        SegmentsOut:        0000000000
  StartDate:          01/09/2012        StartTime:          22:04:11
  Last Touched:       21:41:09          State:              Listen
  RcvNxt:             0000000000        SndNxt:             0000000000
  ClientRcvNxt:       0000000000        ClientSndNxt:       0000000000
  InitRcvSeqNum:      0000000000        InitSndSeqNum:      0000000000
  CongestionWindow:   0000000000        SlowStartThreshold: 0000000000
  IncomingWindowNum:  0000000000        OutgoingWindowNum:  0000000000
  SndWl1:             0000000000        SndWl2:             0000000000
  SndWnd:             0000000000        MaxSndWnd:          0000000000
  SndUna:             0000000000        rtt_seq:            0000000000
  MaximumSegmentSize: 0000000536        DSField:            00
  Round-trip information:
    Smooth trip time: 0.000             SmoothTripVariance: 1500.000
  ReXmt:              0000000000        ReXmtCount:         0000000000
  DupACKs:            0000000000        RcvWnd:             0000032768
  SockOpt:            80                TcpTimer:           00
  TcpSig:             00                TcpSel:             20
  TcpDet:             C0                TcpPol:             00
  TcpPrf:             40
  QOSPolicy:          No
  TTLSPolicy:         No
  RoutingPolicy:      No
  ReceiveBufferSize:  0000016384        SendBufferSize:     0000016384
  ConnectionsIn:      0000000001        ConnectionsDropped: 0000000000
  MaximumBacklog:     0000000010        ConnectionFlood:    No
  CurrentBacklog:     0000000000
    ServerBacklog:    0000000000        FRCABacklog:        0000000000
  CurrentConnections: 0000000001        SEF:                98
  Quiesced:           No
  SharePort: WLM
    RawWeight:        63                NormalizedWeight:   15
    Abnorm:           10                Health:             100
    RawCP:  060       RawzAAP:  000     RawzIIP:  040
    PropCP: 040       PropzAAP: 000     PropzIIP: 023
    ILWeighting: 1    XcostzAAP: 001    XcostzIIP: 001
  Application Data:   EZAFTP0D
----
```

```
Client Name: TCPCS                    Client Id: 0000000C
Local Socket: 9.67.115.5..23          Foreign Socket: 9.27.11.182..4665
  BytesIn:            0000001062        BytesOut:           0000000480
  SegmentsIn:         0000000019        SegmentsOut:        0000000019
  StartDate:          01/09/2012        StartTime:          16:46:15
  Last Touched:       16:46:15          State:              Establsh
  RcvNxt:             3296375906        SndNxt:             3296308452
  ClientRcvNxt:       3296375906        ClientSndNxt:       3296308452
  InitRcvSeqNum:      3296374843        InitSndSeqNum:      3296307971
  CongestionWindow:   0000340353        SlowStartThreshold: 0000016384
  IncomingWindowNum:  3296408638        OutgoingWindowNum:  3296341180
  SndWl1:             3296375906        SndWl2:             3296308452
  SndWnd:             0000032728        MaxSndWnd:          0000032768
  SndUna:             3296308452        rtt_seq:            3296308412
  MaximumSegmentSize: 0000065483        DSField:            00
  Round-trip information:
    Smooth trip time: 37.000            SmoothTripVariance: 101.000
  ReXmt:              0000000000        ReXmtCount:         0000000000
  DupACKs:            0000000000
  SockOpt:            00                TcpTimer:           00
  TcpSig:             00                TcpSel:             C0
  TcpDet:             F0                TcpPol:             00
  TcpPrf:             40
  QOSPolicy:          Yes
    QOSRuleName:      QosRule1
  TTLSPolicy:         Yes
    TTLSRule:         TTLSRule1
    TTLSGrpAction:    TTLSGrpAction1
    TTLSEnvAction:    TTLSEnvAction1
    TTLSConnAction:   TTLSConnAction1 (Stale)
  RoutingPolicy:      Yes
    RoutingTableName: prTabl
    RoutingRuleName:  SecLow2
  ReceiveBufferSize:  0000016384        SendBufferSize:     0000016384
  ReceiveDataQueued:  000000002C
    OldQDate:         09/15/06          OldQTime:           03:36:32
  SendDataQueued:     000002C000
    OldQDate:         09/15/06          OldQTime:           03:36:32
  SendStalled:        No
  SMC information:
    SMCDStatus:        InActive
      SMCReason:   0000530F - Peer did not accept SMC-D request
    SMCRStatus:       Active             SMCGroupId:         00000100
      LocalSMCLinkId:   00000101         RemoteSMCLinkId:    00000301
      LocalSMCRcvBuf:   64K              RemoteSMCRcvBuf:    64K
  Ancillary Input Queue: N/A
  Application Data:   EZBTNSRV TCPM1001 TSO10002 ET ST14S
----
```

```
Client Name: TCPCS1                    Client Id: 0000000D
Local Socket: 9.67.115.5..23          Foreign Socket: 9.27.12.170..4999
  BytesIn:            0000001062        BytesOut:           0000000480
  SegmentsIn:         0000000019        SegmentsOut:        0000000019
  StartDate:          01/09/2012        StartTime:          16:46:15
  Last Touched:       16:46:15          State:              Establsh
  RcvNxt:             3296375906        SndNxt:             3296308452
  ClientRcvNxt:       3296375906        ClientSndNxt:       3296308452
  InitRcvSeqNum:      3296374843        InitSndSeqNum:      3296307971
  CongestionWindow:   0000340353        SlowStartThreshold: 0000016384
  IncomingWindowNum:  3296408638        OutgoingWindowNum:  3296341180
  SndWl1:             3296375906        SndWl2:             3296308452
  SndWnd:             0000032728        MaxSndWnd:          0000032768
  SndUna:             3296308452        rtt_seq:            3296308412
  MaximumSegmentSize: 0000065483        DSField:            00
  Round-trip information:
    Smooth trip time: 37.000            SmoothTripVariance: 101.000
  ReXmt:              0000000000        ReXmtCount:         0000000000
  DupACKs:            0000000000
  SockOpt:            00                TcpTimer:           00
  TcpSig:             00                TcpSel:             C0
  TcpDet:             F0                TcpPol:             00
  TcpPrf:             40
  QOSPolicy:          Yes
    QOSRuleName:      QosRule1
  TTLSPolicy:         Yes
    TTLSRule:         TTLSRule1
    TTLSGrpAction:    TTLSGrpAction1
    TTLSEnvAction:    TTLSEnvAction1
    TTLSConnAction:   TTLSConnAction1 (Stale)
  RoutingPolicy:      Yes
    RoutingTableName: prTabl
    RoutingRuleName:  SecLow2
  ReceiveBufferSize:  0000016384        SendBufferSize:     0000016384
  ReceiveDataQueued:  000000002C
    OldQDate:         09/15/06          OldQTime:           03:36:32
  SendDataQueued:     000002C000
    OldQDate:         09/15/06          OldQTime:           03:36:32
  SendStalled:        No
  SMC information:
    SMCDStatus:        Active
      LocalSMCLinkId:   00000101          RemoteSMCLinkId:    00000301
      LocalSMCRcvBuf:   64K               RemoteSMCRcvBuf:    64K
  Ancillary Input Queue: N/A
  Application Data:   EZBTNSRV TCPM1001 TSO10002 ET ST14S
----
```

```
Client Name: APPV4                    Client Id: 00000015
Local Socket: 0.0.0.0..2049           Foreign Socket: 9.42.103.99..1234
  BytesIn:            0000000200        BytesOut:           0000000100
  DgramIn:            0000000010        DgramOut:           0000000005
  StartDate:          06/16/2011        StartTime:          22:53:55
  Last Touched:       16:00:29
  MaxSendLim:         0000065535        MaxRecvLim:         0000065535
  SockOpt:            00                DSField:            00
  QOSPolicy:          Yes
    QOSRuleName:      QosRule2
  RoutingPolicy:      Yes
    RoutingTableName: prTab4
    RoutingRuleName:  SecLow4
  ReceiveDataQueued:  0000000000        ReceiveMsgCnt:      0000000000
  ----
Client Name: SYSLOGD1                 Client Id: 00000010
Local Socket: 0.0.0.0..514            Foreign Socket: *..*
  BytesIn:            0000000000        BytesOut:           0000000000
  DgramIn:            0000000000        DgramOut:           0000000000
  StartDate:          06/16/2011        StartTime:          23:33:52
  Last Touched:       16:46:29
  MaxSendLim:         0000065535        MaxRecvLim:         0000065535
  SockOpt:            00                DSField:            00
  QOSPolicy:          No
  RoutingPolicy:      No
  ReceiveDataQueued:  0000000000        ReceiveMsgCnt:      0000000000
----
```

IPv6 enabled or request for LONG format

```
NETSTAT ALL
MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           22:06:44
Client Name: FTPD1                    Client Id: 0000006D
  Local Socket: ::1..21
  Foreign Socket: ::1..1026
    BytesIn:            0000000000000000035
    BytesOut:           0000000000000000265
    SegmentsIn:         0000000000000000015
    SegmentsOut:        0000000000000000015
    StartDate:          01/09/2012       StartTime:          22:04:11
    Last Touched:       22:05:51         State:              Establsh
    RcvNxt:             0634886921       SndNxt:             0634950319
    ClientRcvNxt:       0634885851       ClientSndNxt:       0634949426
    InitRcvSeqNum:      0634885815       InitSndSeqNum:      0634949160
    CongestionWindow:   0000299155       SlowStartThreshold: 0000065535
    IncomingWindowNum:  0634919651       OutgoingWindowNum:  0634983003
    SndWl1:             0634886921       SndWl2:             0634950319
    SndWnd:             0000032684       MaxSndWnd:          0000032768
    SndUna:             0634950319       rtt_seq:            0634950235
    MaximumSegmentSize: 0000065463       DSField:            00
    Round-trip information:
      Smooth trip time: 81.000           SmoothTripVariance: 270.000
    ReXmt:              0000000000       ReXmtCount:         0000000000
    DupACKs:            0000000000       RcvWnd:             0000032730
    SockOpt:            8500             TcpTimer:           00
    TcpSig:             85               TcpSel:             64
    TcpDet:             E0               TcpPol:             00
    TcpPrf:             C0               TcpPrf2:            70
    TcpPrf3:            00
    DelayAck:           AutoYes
    QOSPolicy:          No
    TTLSPolicy:         Yes
      TTLSRule:         server
      TTLSGrpAction:    group_action1
      TTLSEnvAction:    Environment1
    RoutingPolicy:      No
    ReceiveBufferSize:  0000016384       SendBufferSize:     0000016384
    ReceiveDataQueued:  0000000000
    SendDataQueued:     0000000000
    SendStalled:        No
    Ancillary Input Queue: Yes
      BulkDataIntfName: OSAQDIO4
    Application Data:   EZAFTP0S C USER1     PTS305
----
```

```
Client Name: US16SVR                  Client Id: 0000000D
Local Socket: 0.0.0.0..10007          Foreign Socket: 0.0.0.0..0
  BytesIn:            0000024000        BytesOut:           0000032000
  SegmentsIn:         0000000900        SegmentsOut:        0000001000
  StartDate:          03/20/2014        StartTime:          17:53:16
  Last Touched:       17:53:16          State:              Listen
  RcvNxt:             0000000000        SndNxt:             0000000000
  ClientRcvNxt:       0000000000        ClientSndNxt:       0000000000
  InitRcvSeqNum:      0000000000        InitSndSeqNum:      0000000000
  CongestionWindow:   0000000000        SlowStartThreshold: 0000000000
  IncomingWindowNum:  0000000000        OutgoingWindowNum:  0000000000
  SndWl1:             0000000000        SndWl2:             0000000000
  SndWnd:             0000000000        MaxSndWnd:          0000000000
  SndUna:             0000000000        rtt_seq:            0000000000
  MaximumSegmentSize: 0000000536        DSField:            00
  Round-trip information:
    Smooth trip time: 0.000             SmoothTripVariance: 1500.000
  ReXmt:              0000000000        ReXmtCount:         0000000000
  DupACKs:            0000000000        RcvWnd:             0000131072
  SockOpt:            00                TcpTimer:           00
  TcpSig:             00                TcpSel:             20
  TcpDet:             C0                TcpPol:             00
  TcpPrf:             00
  QOSPolicy:          No
  RoutingPolicy:      No
  ReceiveBufferSize:  0000065536        SendBufferSize:     0000065536
  ConnectionsIn:      0000000010        ConnectionsDropped: 0000000000
  MaximumBacklog:     0000000004        ConnectionFlood:    No
  CurrentBacklog:     0000000000
    ServerBacklog:    0000000000        FRCABacklog:        0000000000
  CurrentConnections: 0000000005        SEF:                100
  Quiesced:           No
  SMC Information:
    SMCDCurrConns:    0000000002        SMCDTotalConns:     0000000015
    SMCRCurrConns:    0000000004        SMCRTotalConns:     0000000008
    UseSMC:           Yes               Source:             AutoSMC
    AutoSMC%:         090
----
```

```
Client Name: FTPD1                   Client Id: 0000005B
  Local Socket: ::..21
  Foreign Socket: ::..0
    BytesIn:            0000000000000000000
    BytesOut:           0000000000000000000
    SegmentsIn:         0000000000000000000
    SegmentsOut:        0000000000000000000
    StartDate:          01/09/2012       StartTime:          22:05:11
    Last Touched:       22:05:41         State:              Listen
    RcvNxt:             0000000000       SndNxt:             0000000000
    ClientRcvNxt:       0000000000       ClientSndNxt:       0000000000
    InitRcvSeqNum:      0000000000       InitSndSeqNum:      0000000000
    CongestionWindow:   0000000000       SlowStartThreshold: 0000000000
    IncomingWindowNum:  0000000000       OutgoingWindowNum:  0000000000
    SndWl1:             0000000000       SndWl2:             0000000000
    SndWnd:             0000000000       MaxSndWnd:          0000000000
    SndUna:             0000000000       rtt_seq:            0000000000
    MaximumSegmentSize: 0000000536       DSField:            00
    Round-trip information:
      Smooth trip time: 0.000            SmoothTripVariance: 1500.000
    ReXmt:              0000000000       ReXmtCount:         0000000000
    DupACKs:            0000000000       RcvWnd:             0000032768
    SockOpt:            8000             TcpTimer:           00
    TcpSig:             01               TcpSel:             20
    TcpDet:             C0               TcpPol:             00
    TcpPrf:             40
    QOSPolicy:          No
    TTLSPolicy:         No
    RoutingPolicy:      No
    ReceiveBufferSize:  0000016384       SendBufferSize:     0000016384
    ConnectionsIn:      0000000001       ConnectionsDropped: 0000000000
    MaximumBacklog:     0000000010       ConnectionFlood:    No
    CurrentBacklog:     0000000000
      ServerBacklog:    0000000000       FRCABacklog:        0000000000
    CurrentConnections: 0000000001       SEF:                100
    Quiesced:           No
    SharePort: WLM
      RawWeight:        63               NormalizedWeight:   15
      Abnorm:           10               Health:             100
      RawCP:  060       RawzAAP:  000    RawzIIP:  040
      PropCP: 040       PropzAAP: 000    PropzIIP: 023
    Application Data:   EZAFTP0D
----
```

```
Client Name: TCPCS                    Client Id: 0000001E
  Local Socket: 9.67.115.5..23
  Foreign Socket: 9.27.11.182..4665
    BytesIn:            00000000000000001062
    BytesOut:           00000000000000000480
    SegmentsIn:         00000000000000000019
    SegmentsOut:        00000000000000000018
    StartDate:          01/09/2012        StartTime:          14:27:37
    Last Touched:       14:27:37          State:              Establsh
    RcvNxt:             2776729719        SndNxt:             2776682484
    ClientRcvNxt:       2776729719        ClientSndNxt:       2776682484
    InitRcvSeqNum:      2776728656        InitSndSeqNum:      2776682003
    CongestionWindow:   0000340353        SlowStartThreshold: 0000016384
    IncomingWindowNum:  2776762451        OutgoingWindowNum:  2776715212
    SndWl1:             2776729719        SndWl2:             2776682484
    SndWnd:             0000032728        MaxSndWnd:          0000032768
    SndUna:             2776682484        rtt_seq:            2776682444
    MaximumSegmentSize: 0000065483        DSField:            00
    Round-trip information:
      Smooth trip time: 100.000           SmoothTripVariance: 163.000
    ReXmt:              0000000000        ReXmtCount:         0000000000
    DupACKs:            0000000000
    SockOpt:            0000              TcpTimer:           00
    TcpSig:             00                TcpSel:             C0
    TcpDet:             F0                TcpPol:             00
    TcpPrf:             40
    QOSPolicy:          Yes
      QOSRuleName:      QosRule1
    TTLSPolicy:         Yes
      TTLSRule:         TTLSRule1
      TTLSGrpAction:    TTLSGrpAction1
      TTLSEnvAction:    TTLSEnvAction1
      TTLSConnAction:   TTLSConnAction1 (Stale)
    RoutingPolicy:      Yes
      RoutingTableName: prTabl
      RoutingRuleName:  SecLow2
    ReceiveBufferSize:  0000016384        SendBufferSize:     0000016384
    ReceiveDataQueued:  0000000000
    SendDataQueued:     0000000000
    SendStalled:        No
    SMC information:
      SMCDStatus:        Active
        LocalSMCLinkId:   00000101          RemoteSMCLinkId:    00000301
        LocalSMCRcvBuf:   64K               RemoteSMCRcvBuf:    64K
    Ancillary Input Queue: N/A
    Application Data:   EZACICSO CSKL 0000038 CICSUSER CICP
```

```
Client Name: TCPCS                    Client Id: 0000001E
  Local Socket: 9.67.115.5..23
  Foreign Socket: 9.27.11.182..4665
    BytesIn:            0000000000000001062
    BytesOut:           0000000000000000480
    SegmentsIn:         0000000000000000019
    SegmentsOut:        0000000000000000018
    StartDate:          01/09/2012        StartTime:          14:27:37
    Last Touched:       14:27:37          State:              Establsh
    RcvNxt:             2776729719        SndNxt:             2776682484
    ClientRcvNxt:       2776729719        ClientSndNxt:       2776682484
    InitRcvSeqNum:      2776728656        InitSndSeqNum:      2776682003
    CongestionWindow:   0000340353        SlowStartThreshold: 0000016384
    IncomingWindowNum:  2776762451        OutgoingWindowNum:  2776715212
    SndWl1:             2776729719        SndWl2:             2776682484
    SndWnd:             0000032728        MaxSndWnd:          0000032768
    SndUna:             2776682484        rtt_seq:            2776682444
    MaximumSegmentSize: 0000065483        DSField:            00
    Round-trip information:
      Smooth trip time: 100.000           SmoothTripVariance: 163.000
    ReXmt:              0000000000        ReXmtCount:         0000000000
    DupACKs:            00000000000
    SockOpt:            0000              TcpTimer:           00
    TcpSig:             00                TcpSel:             C0
    TcpDet:             F0                TcpPol:             00
    TcpPrf:             40
    QOSPolicy:          Yes
      QOSRuleName:      QosRule1
    TTLSPolicy:         Yes
      TTLSRule:         TTLSRule1
      TTLSGrpAction:    TTLSGrpAction1
      TTLSEnvAction:    TTLSEnvAction1
      TTLSConnAction:   TTLSConnAction1 (Stale)
    RoutingPolicy:      Yes
      RoutingTableName: prTabl
      RoutingRuleName:  SecLow2
    ReceiveBufferSize:  0000016384        SendBufferSize:     0000016384
    ReceiveDataQueued:  0000000000
    SendDataQueued:     0000000000
    SendStalled:        No
    SMC information:
      SMCDStatus:        InActive
        SMCReason:   0000530F - Peer did not accept SMC-D request
      SMCRStatus:       Active             SMCGroupId:         00000100
        LocalSMCLinkId:   00000101          RemoteSMCLinkId:    00000301
        LocalSMCRcvBuf:   64K               RemoteSMCRcvBuf:    64K
    Ancillary Input Queue: N/A
    Application Data:   EZACICSO CSKL 0000038 CICSUSER CICP
```

```
----
Client Name: APPV4                    Client Id: 00000015
  Local Socket: 0.0.0.0..2049
  Foreign Socket: 9.42.103.99..1234
    BytesIn:            00000000000000000200
    BytesOut:           00000000000000000100
    DgramIn:            00000000000000000010
    DgramOut:           00000000000000000005
    StartDate:          06/17/2011        StartTime:          16:00:29
    Last Touched:       16:00:29
    MaxSendLim:         0000065535        MaxRecvLim:         0000065535
    SockOpt:            00000000          DSField:            00
    QOSPolicy:          Yes
      QOSRuleName:      QosRule2
    RoutingPolicy:      Yes
      RoutingTableName: prTab4
      RoutingRuleName:  SecLow4
    ReceiveDataQueued:  0000345655        ReceiveMsgCnt:      0000045644
      OldQDate:         09/15/06          OldQTime:           03:36:32
  Multicast Specific:
    TimeToLive:         0000000001        Loopback:  Yes
    OutgoingIpAddr:     199.1.2.3
    Group             IncomingIpAddr    SrcFltMd
    -----             --------------    --------
    224.8.8.8         193.1.1.94        Exclude
      SrcAddr: 20.20.20.20
               22.22.22.22
----
Client Name: APPV6                    Client Id: 00000016
  Local Socket: ::..2050
  Foreign Socket: 12AB::1..1235
    BytesIn:            00000000000000000200
    BytesOut:           00000000000000000100
    DgramIn:            00000000000000000010
    DgramOut:           00000000000000000005
    StartDate:          06/17/2011        StartTime:          16:00:29
    Last Touched:       16:00:29
    MaxSendLim:         0000065535        MaxRecvLim:         0000065535
    SockOpt:            00000000          DSField:            00
    QOSPolicy:          No
    RoutingPolicy:      No
    ReceiveDataQueued:  0000000000        ReceiveMsgCnt:      0000000000
  Multicast Specific:
    HopLimit:           0000000001        Loopback:  Yes
    OutgoingIntf:
    Group:              ff03::333
      IncomingIntf:     LINK6             SrcFltMd:  Exclude
        SrcAddr:        2e00::7
                        2e00::8
----
Client Name: SYSLOGD1                 Client Id: 0000002C
  Local Socket: 0.0.0.0..529
  Foreign Socket: *..*
    BytesIn:            00000000000000000000
    BytesOut:           00000000000000000000
    DgramIn:            00000000000000000000
    DgramOut:           00000000000000000000
    StartDate:          06/17/2011        StartTime:          14:27:42
    Last Touched:       14:27:42
    MaxSendLim:         0000065535        MaxRecvLim:         0000065535
    SockOpt:            00000000          DSField:            00
    QOSPolicy:          No
    RoutingPolicy:      No
    ReceiveDataQueued:  0000345655        ReceiveMsgCnt:      0000004564
      OldQDate:         09/15/06          OldQTime:           03:36:32
    ReceiveBufferSize:  0000016384        SendBufferSize:     0000016384
----
```

Report field descriptions

- The following fields are displayed for a TCP connection entry:

Client Name
See the Client name or User ID information in Netstat report general concepts for a detailed description.

Client ID
See the Client ID or Connection Number information in Netstat report general concepts for a detailed description.

Local Socket
See the Local Socket information in Netstat report general concepts for a detailed description.

Foreign Socket
See the Foreign Socket information in Netstat report general concepts for a detailed description.

StartDate
Date of the last one of the following events that occurred for the TCP connection or UDP endpoint:

- UDP bind
- TCP bind
- TCP listen
- TCP connection establishment

StartTime
Time of the last one of the following events that occurred for the TCP connection or UDP endpoint:

- UDP bind
- TCP bind
- TCP listen
- TCP connection establishment

BytesIn
The number of bytes of data the stack has received for this connection. This includes both the total bytes that the application has received and the total bytes in the receive buffer that have not yet been read by the application.

Restriction: The TCP/IP stack maintains 64-bit counters for TCP connections and UDP endpoints. However, if you are running an IPv4-only stack, and the Netstat output is in the SHORT format, only the lower 32-bit counter value is displayed. If a large amount of data has been received, the number of bytes can exceed a 32-bit counter so the value displayed will appear to have been reset. Use the FORMAT/-M LONG output option on the Netstat command to cause Netstat to use the LONG format for the output. The LONG format displays the full 64-bit counter value. You can also specify the FORMAT parameter on the IPCONFIG profile statement to set FORMAT LONG as the default value for all Netstat commands.

BytesOut
The number of bytes of data the application has sent. This includes all the data that has been sent to the remote connection and all the data that has not been sent but is buffered and waiting to be sent by the local stack.

Restriction: The TCP/IP stack maintains 64-bit counters for TCP connections and UDP endpoints. However, if you are running an IPv4-only stack, and the Netstat output is in the SHORT format, only the lower 32-bit counter value is displayed. If a large amount of data has been sent, the number of bytes can exceed a 32-bit counter so the value displayed will appear to have been reset. Use the FORMAT/-M LONG output option on the Netstat command to cause Netstat to use the LONG format for the output. The LONG format displays the full 64-bit counter value. You can also specify the FORMAT parameter on the IPCONFIG profile statement to set FORMAT LONG as the default value for all Netstat commands.

SegmentsIn
The number of non-retransmitted TCP packets received for this connection.

Guideline: This value, when displayed for a TCP connection across an SMC-R link, includes the number of Remote Direct Memory Access (RDMA) inbound operations.

SegmentsOut
The number of non-retransmitted TCP packets sent for this connection.

Guideline: This value, when displayed for a TCP connection across an SMC-R link, includes the number of RDMA outbound operations.

Last touched
See the Last touched time information in Netstat report general concepts for a detailed description.

State Describes the state of the TCP connection. See TCP connection status for more information.

RcvNxt
The sequence number of the next byte this side of the connection is expecting to receive. Each byte that is sent or received in a TCP connection has its own unique, ascending sequence number.

SndNxt
The sequence number of the next byte that the stack can send.

ClientRcvNxt
The sequence number of the next byte that the application will read from the receive buffer.

ClientSndNxt
The sequence number of the next byte of data that the application can add to the send buffer.

InitRcvSeqNum
The first sequence number that was received from the remote stack host when establishing the connection.

InitSndSeqNum
The first sequence number that the local stack sent out when establishing the connection.

CongestionWindow
The value that is used when congestion is detected in the network to limit the amount of data that is sent by the local stack. This value

represents the maximum amount of data that is sent without waiting for an acknowledgment from the remote socket.

SlowStartThreshold
The slow-start threshold is used to determine whether the connection is recovering from congestion. If the congestion window is smaller than the slow-start threshold, the connection will take actions to more quickly recover from congestion.

IncomingWindowNum
The incoming window number is the maximum sequence number that the remote socket can send until the local application reads more data from the local socket.

OutgoingWindowNum
The outgoing window number is the maximum sequence number that can be sent without waiting for the remote socket to read data (see the send window).

SndWl1
The sequence number from the segment that last updated the SndWnd field.

SndWl2
The acknowledgment number from the segment that last updated the SndWnd field.

SndWnd
The amount of available buffer space that is advertised by the remote side into which data can be sent.

MaxSndWnd
The largest send window the remote socket has sent to the local socket.

SndUna
This value is the sequence number of the first byte of data in the local socket's send buffer that has not been acknowledged by the remote socket.

rtt_seq
The sequence number of the byte of data sent in a packet for which the local socket is measuring the round-trip time (the time it takes between the local socket sending a packet and receiving an acknowledgment from the remote socket).

MaximumSegmentSize
The largest amount of data the local socket can send in a single packet.

DSField
The Differentiated Services Code Point value being used for this connection.

The DSField represents one of the following values:

- If there is a Service Policy Agent policy in effect for this entry, one of the following values is used:
  - The ToS value defined by RFC 791 and RFC 1349.
  - The Differentiated Services field value defined by RFC 2474.
- If there is no Service Policy Agent policy in effect for this entry, the value is 0.

Round-trip information
The round-trip time is the amount of time that elapses between the time a packet is sent and the time an acknowledgment for that packet is received.

Smooth trip time
The average amount of time it has taken for a packet to be sent and an acknowledgment to be received for this connection, measured in milliseconds.

SmoothTripVariance
The average variation in round-trip time, measured in milliseconds.

ReXmt
The total number of times a packet has been retransmitted for this connection. This count is historical for the life of the connection.

ReXmtCount
The number of times the last packet that was sent has been retransmitted.

DupACKs
The total number of duplicate acknowledgments that have been received by this connection.

RcvWnd
The amount of available buffer space that is advertised to the remote side into which data can be received.

SockOpt
Socket option flag. For TCP/IP stacks that are not IPv6 enabled, it is a one-byte hexadecimal value of common socket options. For IPv6-enabled TCP/IP stacks, it is a one-byte hexadecimal value of common socket options, followed by a one-byte hexadecimal value of IPv6-specific socket options.

Common socket options:

80 1... ....
Indicates that the socket option SO_REUSEADDR has been set for this socket. This socket option allows the socket to be bound to the same port that other sockets are bound to.

40 .1.. ....
Indicates that the socket option SO_OOBINLINE has been set for this socket. If this socket option is set, out-of-band data is returned in a normal read operation. If this socket option is not set, out-of-band data can be retrieved only by setting the MSG_OOB flag on a read operation.

20 ..1. ....
Indicates that the socket option SO_LINGER has been set for this socket. The SO_LINGER socket option allows an application to specify whether unsent data is discarded when the socket is closed, and how long to wait if the data is not discarded.

10 ...1 ....
Indicates that the socket option SO_DONTROUTE has been set for this socket. If this socket option is set, data is sent without regard to routes. This is equivalent to the MSG_DONTROUTE flag on a write operation.

08 .... 1...
Indicates the socket option TCP_NODELAY has been set for this socket. Unless this socket option is set, the TCP/IP stack will attempt to optimize the sending of small data packets by holding them briefly in case it has more data to send.

04 .... .1..
Indicates that the SO_KEEPALIVE socket option has been set for this socket. If this socket option is set, the TCP/IP stack will periodically send empty packets to the remote stack to make sure the connection is still alive.

IPv6 socket options:

80 1... ....
Indicates that the IPV6_UNICAST_HOPS option has been set for this socket.

20 ..1. ....
Indicates that the IPV6_USE_MIN_MTU for unicast option has been set for this socket.

10 ...1 ....
Indicates that the IPV6_TCLASS option has been set for this socket.

08 .... 1...
Indicates that the IPV6_RECVTCLASS option has been set for this socket.

04 .... .1..
Indicates that the IPV6_RECVHOPLIMIT option has been set for this socket.

02 .... ..1.
Indicates that the IPV6_V6ONLY option has been set for this socket.

Any other value
Used for diagnostic purposes only under the direction of IBM Service personnel.

TcpTimer
TCP timer flag. It is a one-byte hexadecimal value that is used for diagnostic purposes only under the direction of IBM Service personnel.

TcpSig
TCP signal flag. It is a one-byte hexadecimal value and can have one of the following values:

80 1... ...
Indicates the application has requested to receive the SIGURG signal when urgent data is received on this socket.

40 .1.. ....
Indicates the application has requested to receive the SIGIO signal when data is received on this socket.

Any other value
Is used for diagnostic purposes only under the direction of IBM Service personnel.

TcpSel TCP select flag. It is a one-byte hexadecimal value that is used for diagnostic purposes only under the direction of IBM Service personnel.

TcpDet
Special TCP protocol flag. It is a one-byte hexadecimal value:

04 .... .1..
Indicates the TCP_KEEPALIVE socket option has been set for this socket. This socket option is used to set a socket-specific time interval value for use with the SO_KEEPALIVE socket option. See the description of field SockOpt for an explanation of the SO_KEEPALIVE socket option. The TCP_KEEPALIVE time interval value is in effect only if the SO_KEEPALIVE socket option is set for the socket.

Any other value
Is used for diagnostic purposes only under the direction of IBM Service personnel.

TcpPol
TCP poll flag. It is a one-byte hexadecimal value to be used for diagnostic purposes only under the direction of IBM Service personnel.

TcpPrf A 1-byte hexadecimal TCP performance flag that can have any ofthe following values:

80 1... ....
Indicates that this connection is eligible for dynamic right sizing (DRS) optimization support. For more information about DRS, see TCP receive window in z/OS Communications Server: IP Configuration Guide.

40 .1.. ....
Indicates that DRS is active for this connection so that the stack automatically tunes the receive buffer size. The ReceiveBufferSize field shows the current size of the receive buffer for this connection.

02 .... ..1.
Indicates that DRS was active for this connection, but has been disabled. This is caused by the associated application not reading the data as fast as the data arrives and CSM high virtual common or fixed storage being constrained.

Any other value
Used for diagnostic purposes only under the direction of IBM Service personnel.

TcpPrf2
A 1-byte hexadecimal TCP performance flag that can have any of the following values:

40 ..1. ....
If outbound right sizing (ORS) is active for this connection, the stack expanded the send buffer beyond its original size. For more information about ORS, see TCP send window in z/OS Communications Server: IP Configuration Guide.

20 ..1. ....
Indicates that this connection is eligible for ORS optimization support.

10 ...1 ....
Indicates that ORS is active for this connection so that the stack automatically tunes the send buffer size. The SendBufferSize field shows the current size of the send buffer for this connection.

Any other value
Used for diagnostic purposes only under the direction of IBM Service personnel.

TcpPrf3
Used for diagnostic purposes only under the direction of IBM Service personnel.

DelayAck
Indicates how the TCP/IP stack controls the transmission of acknowledgments for packets received with the PUSH bit on in the TCP header. This field can have the following values:

AutoYes
The TCP/IP stack has autonomically determined to delay transmission of acknowledgments for packets received with the PUSH bit on in the TCP header.

Yes
The TCP/IP stack delays transmission of acknowledgments for packets received with the PUSH bit on in the TCP header.

AutoNo
The TCP/IP stack has autonomically determined to immediately return acknowledgments for packets received with the PUSH bit on in the TCP header.

No The TCP/IP stack immediately returns acknowledgments for packets received with the PUSH bit on in the TCP header.

QOSPolicy
Indicates whether a matching QoS policy rule has been found for this connection. This field can have the following values:

No Indicates that a matching QoS policy rule was not found for this connection.

Yes
Indicates that a matching QoS policy rule was found for this connection. When the QOSPolicy field has the value `Yes`, the following information is displayed:

QOSRuleName
The name of the Policy rule that is in use for this connection. This policy is for outbound traffic only.

TTLSPolicy
Indicates whether a matching Application Transparent Transport Layer Security (AT-TLS) policy rule has been found for this connection. This set of fields is not displayed if the AT-TLS function was disabled when the connection was established (NOTTLS was specified on the TCPCONFIG statement or is in effect by default) or policy lookup has not yet occurred.

– **TTLSPolicy: No** indicates that no matching AT-TLS policy rule was found for this connection. There is no rule or action listed.

– **TTLSPolicy: Yes** indicates one of the following cases:
  - A matching AT-TLS policy rule was found for this connection with an indication that AT-TLS should be enabled (TTLSEnabled ON was specified on the TTLSGroupAction). The rule and actions are displayed.
  - A matching AT-TLS policy rule was found for this connection with an indication that AT-TLS should be disabled (TTLSEnabled OFF was specified on the TTLSGroupAction). The rule and actions are displayed.

TTLSRule
The name of the AT-TLS policy rule that is in use for this connection, followed by `(Stale)` when the rule is no longer available for use by new connections. This field is not displayed when the connection does not match a policy rule.

TTLSGrpAction
The name of the AT-TLS policy group action that is in use for this connection, followed by `(Stale)` when the action is no longer available for use by new connections. This field is not displayed when the connection does not match a policy rule.

TTLSEnvAction
The name of the AT-TLS policy environment action that is in use for this connection, followed by `(Stale)` when the action is no longer available for use by new connections. This field is not displayed when the connection does not match a policy rule or when no TTLSEnvironmentAction was specified.

TTLSConnAction
The name of the AT-TLS policy connection action that is in use for this connection, followed by `(Stale)` when the action is no longer available for use by new connections. This field is not displayed when the connection does not match a policy rule or when no TTLSConnectionAction was specified.

RoutingPolicy
Indicates whether a matching routing policy rule has been found for this connection. This field can have the following values:

No Indicates that no matching routing policy rule was found for this connection.

For an Enterprise Extender (EE) UDP socket entry, the RoutingPolicy value is always `No`. Display the routing policy information for an Enterprise Extender (EE) UDP socket entry by using the DISPLAY NET,EEDIAG,TEST=YES command. See z/OS Communications Server: SNA Operation for details.

Yes Indicates that a matching routing policy rule was found for this connection.

When the RoutingPolicy value is `Yes`, the following information is displayed:

RoutingTableName
The name of the routing table that was used to find the route for this connection or `*NONE*` if a route was not found. The value `EZBMAIN` is displayed when the main routing table was used.

RoutingRuleName
The name of the routing policy rule in use for this connection.

ReceiveBufferSize
The number of bytes received from the remote application that this connection is allowed to maintain in a buffer. All the data that is received is kept in a buffer until the local application reads the data.

SendBufferSize
The number of bytes the local application has sent that this connection is allowed to maintain in a buffer. All data that the application has sent is kept in the buffer until the remote side acknowledges receiving the sent data.

TcpClusterConnFlag
TCP cluster connection type flag. It is a one-byte hexadecimal field and can have one of the following values:

80 1... ....
Indicates that the SO_CLUSTERCONNTYPE socket option or the SIOCGPARTNERINFO ioctl was requested.

08 .... 1...
If the SO_CLUSTERCONNTYPE socket option or the SIOCGPARTNERINFO ioctl was issued for this socket, this bit indicates that the communication from this node to the stack hosting the partner application is not sent on links/interfaces exposed outside the cluster (sysplex).

04 .... .1..
If the SO_CLUSTERCONNTYPE socket option or the SIOCGPARTNERINFO ioctl was issued for this socket, this bit indicates that the connection partners are in the same MVS image.

02 .... ..1.
If the SO_CLUSTERCONNTYPE socket option or the SIOCGPARTNERINFO ioctl was issued for this socket, this bit indicates that the connection partners are in the same cluster.

01 1
If the SO_CLUSTERCONNTYPE socket option or the SIOCGPARTNERINFO ioctl was issued for this socket, this bit indicates that the connection partners are not in the same cluster.

00 ....
If the TcpTrustedPartner flag indicates that the SIOCSPARTNERINFO ioctl has been successfully issued or inherited from the listener socket, this value indicates that the SO_CLUSTERCONNTYPE socket option or the SIOCGPARTNERINFO ioctl has not been issued for this socket.

Any other value
Used for diagnostic purposes only under the direction of IBM Service personnel.

For more information about the cluster connection type, see the z/OS Communications Server: IP Sockets Application Programming Interface

Guide and Reference. For more information about the SIOCGPARTNERINFO ioctl, see z/OS Communications Server: IP Programmer's Guide and Reference.

TcpTrustedPartner
The TCP trusted connection flag is displayed in the following situations:

- Security credentials of a partner within a sysplex or subplex have been retrieved over a trusted TCP connection using the SIOCGPARTNERINFO ioctl.
- The SIOCSPARTNERINFO ioctl has been issued for the socket.

The TCP trusted connection flag is a 1-byte hexadecimal field and can have the following values:

80 1... ....
This bit indicates that the partner address-space user ID has been retrieved, as well as the task-level user ID if it is available.

40 .1.. ....
This bit indicates that the partner address-space UTOKEN has been retrieved, as well as the task-level UTOKEN if it is available.

20 ..1. ....
This bit indicates that the SIOCSPARTNERINFO ioctl has been successfully issued or inherited from the listener socket.

For information about trusted TCP/IP connections and the SIOCGPARTNERINFO and SIOCSPARTNERINFO ioctl calls, see z/OS Communications Server: IP Programmer's Guide and Reference.

ReceiveDataQueued
The number of bytes of data on the receive queue from the remote application yet to be read. This field is not displayed for a connection that is in listen state. The amount of data queued can be up to double the ReceiveBufferSize size. When the number of bytes is not zero, the following information is displayed:

OldQDate
The date of the oldest data on the receive queue.

OldQTime
The time of the oldest data on the receive queue. This value does not include leap seconds.

The ReceiveDataQueued information is not displayed for a connection that is in listen state.

SendDataQueued
The number of bytes of data on the send queue waiting for the remote side to acknowledge. This field is not displayed for a connection that is in listen state. The amount of data queued can be up to double the size of the SendBufferSize. When the number of bytes is not zero, the following information is displayed:

OldQDate
The date of the oldest data on the send queue.

OldQTime
The time of the oldest data on the send queue. This value does not include leap seconds.

The SendDataQueued information is not displayed for a connection that is in listen state.

SendStalled

Indicates whether this connection's send data flow is stalled. The send data flow is considered stalled if one or more of the following conditions are true:

– The TCP send window size is less than 256 or is less than the smaller of the largest send window that has been seen for the connection and the default MTU. The TCP send window size is set based on values provided by the TCP peer. The default MTU for IPv4 is 576. The default MTU for IPv6 is 1280.

– The TCP send queue is full and the data is not being retransmitted.

This field is not displayed for a connection that is in listen state. If the value is Yes, then this connection's send data flow is stalled.

SMC Information

– For server connections, this section is the SMC information for connections in Listen state. This section is displayed for connections in one of the following situations:

- At least one Peripheral Component Interconnect Express® (PCIe) function ID (PFID) was defined by using the SMCR parameter of the GLOBALCONFIG statement.
- The SMCD parameter was defined in the GLOBALCONFIG statement.

The SMC Information section contains the following information that is related to inbound connections to the server application:

SMCDCurrConns

The number of currently established connections, which use SMC-D and have an SMCDStatus of Active, to this server. The value of SMCDCurrConns is a subset of the value of the CurrentConnections field in this report.

SMCDTotalConns

The total number of connections to this server that uses SMC-D. The value of SMCDTotalConns is a subset of the value of the ConnectionsIn field in this report.

SMCRCurrConns

The number of currently established connections with an SMCRStatus of Active to this server that uses SMC-R. The value of SMCRCurrConns is a subset of the value of the CurrentConnections field in this report.

SMCRTotalConns

The total number of connections to this server that uses SMC-R. The value of SMCRTotalConns is a subset of the value of the ConnectionsIn field in this report.

UseSMC

Indicates whether SMC is used. This field is displayed only for a connection that is in Listen state when the AUTOSMC monitoring function is enabled. The AUTOSMC monitoring function is enabled by specifying the AUTOSMC subparameter of the SMCGLOBAL parameter on the GLOBALCONFIG profile statement. The AUTOSMC

subparameter of the SMCGLOBAL parameter on GLOBALCONFIG is the default setting. For more information about the AUTOSMC monitoring function, see AUTOSMC monitoring function in z/OS Communications Server: IP Configuration Guide.

Guideline: A client is best suited for both SMC-R and SMC-D communications, or is best suited for neither of the communications. The workload pattern criteria are the same for determining whether a client is best suited for SMC-R and SMC-D communications.

Yes Indicates one of the following situations:

- This server had SMC configured on its PORT or PORTRANGE statement.
- The AUTOSMC monitoring function detected during the previous monitoring interval that most client connections that request SMC-R or SMC-D to this server had a workload pattern that was best suited for SMC communications.

No Indicates one of the following situations:

- This server had NOSMC configured on its PORT or PORTRANGE statement.
- The AUTOSMC monitoring function detected during the previous monitoring interval that most client connections that request SMC-R or SMC-D to this server did not have a workload pattern that was best suited for SMC communications.

Source

Indicates how the value of UseSMC is determined. This field is displayed only for a connection that is in Listen state when the AUTOSMC monitoring function is enabled. The AUTOSMC monitoring function is enabled by specifying the AUTOSMC subparameter of the SMCGLOBAL parameter on the GLOBALCONFIG profile statement. The AUTOSMC subparameter of the SMCGLOBAL parameter on GLOBALCONFIG is the default setting. For more information about the AUTOSMC monitoring function, see AUTOSMC monitoring function in z/OS Communications Server: IP Configuration Guide.

AUTOSMC
Indicates that the value of UseSMC was determined by the AUTOSMC monitoring function.

Config
Indicates that the value of UseSMC was determined by the configuration of the PORT or PORTRANGE statement for the server.

AutoSMC%

The percentage of inbound TCP connections that request SMC-R or SMC-D to this server that had a workload pattern best suited for SMC communications during the last AUTOSMC monitoring interval. An N/A will be displayed if the number of connections to analyze in the last monitored

interval is not large enough. Only connections that meet the criteria for SMC-R or SMC-D enablement are monitored. These connections where the peers are SMC-R or SMC-D enabled, can be reached directly over an SMC-R or SMC-D eligible subnet, do not have IPSEC enabled, and do not exploit the Fast Response Cache Accelerator (FRCA) feature. This field is only displayed when the AUTOSMC monitoring function is enabled and Source is AutoSMC. The AUTOSMC monitoring function is enabled by the AUTOSMC subparameter of the SMCGLOBAL parameter on the GLOBALCONFIG profile statement. The AUTOSMC subparameter of the SMCGLOBAL parameter on GLOBALCONFIG is the default setting.

Guideline: A client is best suited for both SMC-R and SMC-D communications, or is best suited for neither of the communications. The workload pattern criteria are the same for determining whether a client is best suited for SMC-R and SMC-D communications.

– For client connections, this section is the SMC information for established connections. This section is displayed for connections in one of the following situations:
  - At least one Peripheral Component Interconnect Express (PCIe) function ID (PFID) was defined by using the SMCR parameter of the GLOBALCONFIG statement.
  - The SMCD parameter was defined in the GLOBALCONFIG statement.

  The SMC Information section contains the following information:

  SMCDStatus
  Indicates whether this connection is traversing a Shared Memory Communications - Direct Memory Access (SMC-D) link. This field can have the following values:

  Inactive
  Indicates that this connection does not use an SMC-D link.

  When the `SMCDStatus` value is `Inactive`, the following information is displayed:

  SMCReason *reasonCode - reasonText*
  This field explains why the connection is not using an SMC-D link. The following reason codes are possible values.

  Note: An asterisk (*) might be displayed after the reason code value, for example, 5302*. The asterisk indicates that a previous attempt to establish an SMC-D link to the destination IP address failed and that TCP/IP cached this failure. Therefore, TCP/IP did not attempt to use SMC-D for this connection. For more information about SMC-D caching, see GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference.

5302 - Route not SMC eligible
SMC-D communications cannot be used for this connection because of connectivity issues or the absence of an active interface that supports SMC-D processing.

5306 - No storage for SMC negotiation
Storage for SMC-D negotiation over this TCP connection cannot be obtained.

5307 - Connection uses lPSec
SMC-D communications cannot be used for this connection because the connection is using IP security.

5308 - FRCA server
SMC-D communications cannot be used for this connection because the connection is used by a Fast Response Cache Accelerator (FRCA) server.

5309 - Pascal application
SMC-D communications cannot be used because the connection is used by a Pascal API application.

530A - NOSMC Port server
SMC-D communications cannot be used for this connection because the server port was configured with the NOSMC option.

530C - No prefix on interface
SMC-D communications cannot be used for this connection because of no valid IPv6 prefixes for the associated OSD or HiperSockets interface.

530D - AUTOSMC detected workload
SMC-D communications cannot be used for this connection because of AUTOSMC monitoring. AUTOSMC monitoring detects whether SMC-D is suitable for workload on inbound connections to a particular server. For more information about the AUTOSMC monitoring function, see AUTOSMC monitoring function in z/OS Communications Server: IP Configuration Guide.

530E - No active ISMs for the PNetID
No active Internal Shared Memory (ISM) interface is detected for the PNetID.

530F - Peer did not accept SMC-D request
The remote connection peer is not configured to use SMC-D communications.

5708 - Peer not reachable for SMC-D
The peer host supports SMC-D, but the peer is not reachable via SMC-D. For example, the peer might be located on a different CEC, the peer might not have SMC-D enabled for the same PNetID, or the defined VLANs for SMC-D are not consistent on both peers.

5803 - Insufficient virtual storage
SMC-D communications cannot be used for this connection because TCP private 64-bit virtual storage could not be allocated for a direct memory buffer (DMB).

5804 - SMCD FIXEDMemory limit exceeded reached
SMC-D communications cannot be used for this connection because the required SMC-D memory could not be allocated.

5805 - TCP connection limit reached
SMC-D communications cannot be used for this connection because another DMB for a new connection could not be obtained.

5806 - VLAN ID not found
SMC-D communications cannot be used for this connection because no VLAN that SMC-D enabled was found.

5809 - No qualifying active ISMs
No active ISM interfaces are detected in the SMC-D layer that can be used for this TCP connection.

5819 - Peer is out of synch
SMC-D communications cannot be used for this connection because of a condition that the peer is out of synchronization during negotiation.

581E - Peer subnet/prefix mismatch
SMC-D communications cannot be used for this connection because the peer does not have an active interface in the same subnet that is eligible for SMC-D.

reasonCode **- Internal error**
SMC-D communications cannot be used for this connection because of an internal error.

reasonCode **- *Peer generated***
SMC-D communications cannot be used for this connection because the peer reported an error. See the peer product's documentation for additional details. A value of NA indicates that the TCP/IP stack could not obtain the reason code from the peer.

Active Indicates that this connection uses an SMC-D link.

When the `SMCDStatus` value is `Active`, the following information is displayed and the SMCRStatus field is not displayed:

LocalSMCLinkId
This field identifies the SMC-D link on this TCP/IP stack that this connection traverses. This TCP/IP stack generates the SMC-D link identifier dynamically.

RemoteSMCLinkId
This field identifies the SMC-D link on the remote peer that this connection traverses. The remote peer generates this SMC-D link identifier and provides it to this TCP/IP stack during SMC-D link activation.

LocalSMCRcvBuf
This field indicates the size of the DMB element that the local host uses for receiving data on this connection from the remote host.

RemoteSMCRcvBuf
This field indicates the size of the DMB element that the remote host uses for receiving data on this connection from the local host.

SMCRStatus
Indicates whether this connection is traversing a Shared Memory Communications over Remote Direct Memory Access (SMC-R) link. This field can have the following values:

Inactive
Indicates that this connection does not use an SMC-R link.

When the `SMCRStatus` value is `Inactive`, the following information is displayed:

SMCReason *reasonCode - reasonText*
This field explains why the connection is not using an SMC-R link. The following reason codes are possible values.

Note: An asterisk (*) might be displayed after the reason code value, for example, 5013*. The asterisk indicates that a previous attempt to establish an SMC-R link to the destination IP address failed and that TCP/IP cached this failure. Therefore, TCP/IP did not attempt to use SMC-R for this connection. For more information about SMC-R caching, see GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference.

5013 - RDMA connectivity failure
SMC-R communications cannot be used for this connection because the first attempt to send data over RDMA encountered an error. A likely reason for this error is a configuration problem in the switch that is connected to the RoCE Express interface. For example, an incorrect VLANID value was configured on the switch port for the RoCE Express interface.

5203 - Insufficient virtual storage
SMC-R communications cannot be used for this connection because TCP private 64-bit virtual storage could not be allocated for an RMB buffer.

5204 - SMCR FIXEDMemory limit exceeded reached
SMC-R communications cannot be used for this connection because the required SMC-R memory could not be allocated.

5205 - TCP connection limit reached
SMC-R communications cannot be used for this connection because another RMB for a new connection could not be obtained.

5206 - VLAN ID not found
SMC-R communications cannot be used for this connection because no VLAN that was enabled by SMC-R was found.

5209 - No qualifying active RNICs
No active IBM 10GbE RoCE Express interfaces are detected in the SMC-R layer that can be used for this TCP connection.

5219 - Peer is out of synch
SMC-R communications cannot be used for this connection because the

peer is out of synchronization condition during negotiation.

521E - Peer subnet/prefix mismatch
SMC-R communications cannot be used for this connection because the peer does not have an active interface in the same subnet that is eligible for SMC-R.

5301 - Peer did not accept SMC-R request
The remote connection peer is not configured to use SMC-R communications.

5302 - Route not SMC eligible
SMC-R communications cannot be used for this connection because of connectivity issues or the absence of an active interface that supports SMC-R processing.

5303 - No active RNICs for the PNetID
No active 10GbE RoCE Express features are detected for the PNetID.

5304 - Connection is local
The connection peers are on the same TCP/IP stack.

5306 - No storage for SMC negotiation
Storage for SMC-R negotiation over this TCP connection cannot be obtained.

5307 - Connection uses lPSec
SMC-R communications cannot be used for this connection because the connection is using IP security.

5308 - FRCA server
SMC-R communications cannot be used for this connection because the connection is used by a Fast Response Cache Accelerator (FRCA) server.

5309 - Pascal application
SMC-R communications cannot be used because the connection is used by a Pascal API application.

530A - NOSMC Port server
SMC-R communications cannot be used for this connection because the server port was configured with the NOSMC option.

530B - Invalid MTU from peer
SMC-R communications cannot be

used for this connection because the peer had an invalid MTU size for this SMC-R link.

530C - No prefix on interface
SMC-R communications cannot be used for this connection because of no valid IPv6 prefixes for the associated OSD interface.

530D - AUTOSMC detected workload
SMC-R communications cannot be used for this connection because of AUTOSMC monitoring. AUTOSMC monitoring detects whether SMC-R is suitable for workload on inbound connections to a particular server. For more information about the AUTOSMC monitoring function, see AUTOSMC monitoring function in z/OS Communications Server: IP Configuration Guide.

reasonCode **- Internal error**
SMC-R communications cannot be used for this connection because of an internal error.

reasonCode **- *Peer generated***
SMC-R communications cannot be used for this connection because the peer reported an error. See the peer product's documentation for additional details.

Active Indicates that this connection uses an SMC-R link.

When the `SMCRStatus` value is `Active`, the following information is displayed:

SMCGroupId
This field identifies the SMC-R link group that includes the individual SMC-R link that this connection traverses. This TCP/IP stack generates the SMC-R link group identifier dynamically.

LocalSMCLinkId
This field identifies the SMC-R link on this TCP/IP stack that this connection traverses. This TCP/IP stack generates the SMC-R link identifier dynamically.

RemoteSMCLinkId
This field identifies the SMC-R link on the remote peer that this connection traverses. The remote peer generates this SMC-R link identifier and provides it to this TCP/IP stack during SMC-R link activation.

LocalSMCRcvBuf
This field indicates the size of the RMB element that the local host uses for receiving data on this connection from the remote host.

RemoteSMCRcvBuf
This field indicates the size of the RMB element that the remote host uses for receiving data on this connection from the local host.

Ancillary Input Queue
Indicates whether this connection is registered to the TCP bulk data ancillary input queue. This field is not displayed for a connection that is in listen state. This field can have the following values:

N/A Indicates that this connection is not registered to the TCP bulk data ancillary input queue.

Yes Indicates that this connection is registered to the TCP bulk data ancillary input queue.

When the Ancillary Input Queue value is Yes, the following information is displayed:

BulkDataIntfName
This field indicates the name of the interface over which the inbound traffic is being received.

ConnectionsIn
The number of connections that a server has accepted. This field is displayed only for a connection that is in listen state. Once a connection has been accepted, communication can begin between the client and server applications.

ConnectionsDropped
The number of connection requests that have been received by the server and dropped because the maximum number of connection requests was already in the backlog queue. This field is displayed only for a connection that is in listen state.

MaximumBacklog
The maximum number of connections that a server maintains on the backlog queue. This field is displayed only for a connection that is in listen state. Connection requests that are received when the maximum number of connections requests is already on the backlog queue are typically discarded. A high maximum backlog queue value causes more simultaneous connection requests than a server can handle without having to drop requests.

ConnectionFlood
Indicates whether this server is experiencing a potential connection flood attack. A server is considered under a potential connection flood attack when backlog queue expansion is required to handle the incoming connection requests. The point where a potential connection flood attack is detected is based on the initial size of the backlog queue. A small initial backlog queue (for example, 10 entries) is allowed to expand twice before the server is considered under attack, while a server with a large initial backlog queue (for example, 500 entries) can expand once, up to a maximum of 768 entries, before it is considered under attack. This field

is displayed only for a connection that is in listen state. If the value is Yes, then this server is experiencing a potential connection flood attack.

CurrentBacklog
The number of connections that are currently in the backlog queue. This field is displayed only for a connection that is in listen state. This value includes connections that are fully established and that are ready to be accepted by the server application; it also includes connections that are not yet fully established (the TCP connection establishment handshake is not yet complete). To determine the number of connections in the backlog queue that are not fully established, subtract the ServerBacklog value from the CurrentBacklog value. If the server application uses the Fast Response Cache Accelerator (FRCA) feature, fully established connections that are being serviced by TCP/IP from the FRCA cache are also included in the CurrentBacklog value. The FRCABacklog value in this report indicates the number of these connections.

ServerBacklog
The number of connections currently in the backlog queue that are established and that have not yet been accepted.

FRCABacklog
The number of connections currently in the backlog queue that are established FRCA connections and that are being serviced by TCP/IP from the FRCA cache. These connections do not need to be accepted by the server application. This field is applicable only for server applications that use the FRCA feature.

CurrentConnections
The number of currently established connections to the server. This field is displayed only for a connection that is in listen state.

SEF The server accept efficiency fraction (SEF) is a measure, calculated at intervals of approximately one minute, of the efficiency of the server application in accepting new connection setup requests and managing its backlog queue. The value is displayed as a percentage. A value of 100 indicates that the server application is successfully accepting all its new connection setup requests. A value of 0 indicates that the server application is not responding to new connection setup requests. This field is displayed only for a connection that is in listen state.

When using SHAREPORTWLM, the SEF value is used to modify the WLM server-specific weights, thereby influencing how new connection setup requests are distributed to the servers sharing this port. When using SHAREPORT, the SEF value is used to weight the distribution of new connection setup requests among the SHAREPORT servers. Whether SHAREPORT or SHAREPORTWLM are specified, the SEF value is reported back to the distributor to be used as part of the target server responsiveness fraction calculation, which influences how new connection setup requests are distributed to the target servers.

Quiesced
Indicates whether this server application has been quiesced for DVIPA sysplex distributor workload balancing. This field is displayed only for a connection that is in listen state. If the value is Dest, then this server will receive no new DVIPA sysplex distributor workload connections until the server application has been resumed. When the server application is resumed, the quiesced value changes to No.

SharePort

Indicates that multiple TCP listening servers are sharing the same port. This field is displayed only for a connection that is in listen state. The method used by TCP to distribute incoming connections to the listeners is indicated by Base or WLM described below. See the PORT profile statement in the z/OS Communications Server: IP Configuration Reference for more information on sharing a TCP port.

Base Connections are proportionally distributed among the available shareport listeners using the SEF value. This value corresponds to the SHAREPORT parameter on the PORT profile statement.

WLM Connections are distributed among the available shareport listeners using the normalized WLM server-specific weights. This value corresponds to the SHAREPORTWLM parameter on the PORT profile statement.

RawWeight

The raw composite weight for this server. The composite weight is based on the application's general CPU, zAAP, and zIIP processor utilization.

NormalizedWeight

The normalized values of the WLM server-specific weights. The original raw weights received from WLM are proportionally reduced for use by the distribution algorithm. Connections are distributed to these servers in a weighted round-robin fashion using the normalized weights if SHAREPORTWLM is specified on the PORT profile statement. The displayed normalized weight is shown after it has been modified by the SEF value. This field is shown regardless of the distribution method (Base or WLM) that is used.

Abnorm

Indicates whether the server application is experiencing conditions that cause transactions to complete abnormally. The value represents a rate of abnormal transaction completions per 1000 total transaction completions. It is applicable only for TCP applications that act as Subsystem Work Managers and report transaction status using Workload Management Services, such as IWMRPT. For example, the value 100 indicates that 10% of all transactions processed by the server application are completing abnormally. Under normal conditions, this value is 0. A nonzero value indicates that the server application has reported some abnormal transactions completions to WLM and that WLM has reduced the recommendation provided to sysplex distributor for this server instance. This reduction in the WLM recommendation enables more new TCP connections to be directed to servers that are not experiencing problem conditions that lead to abnormal transaction completions.

The greater the Abnorm rate field value, the greater the reduction WLM applies to the recommendation for this target instance. For more information about the conditions that cause the abnormal transaction completions for a given server application, see the documentation provided by the server application.

If applications do not provide this transaction status to WLM or SHAREPORTWLM is not configured, then this field has the value 0. For more information about workload management interfaces, see z/OS MVS Programming: Workload Management Services.

Health
The server application health indicator. This health indicator is available only for applications that provide this information to WLM using the IWM4HLTH or IWMSRSRG services. It provides a general health indication for an application or subsystem. Under normal circumstances, the value of this field is 100, indicating that the server is 100% healthy. Any value that is less than 100 indicates that the server is experiencing problem conditions that might prevent new work requests from being successfully processed. A value of less than 100 also causes the WLM to reduce the recommendation provided to the sysplex distributor for this server instance. This reduction in the WLM recommendation enables more new TCP connections to be directed to servers that are not experiencing problem conditions.

The reduction in the WLM recommendation is proportional to value of the Health indicator. For example, if the health value is 20%, WLM reduces the recommendation for this server by 80%. For more information about the conditions leading to a health indicator of less than 100, see the documentation for the server application.

If applications do not provide this health indicator to WLM or SHAREPORTWLM is not configured, then the value of this field is 100. For more information about workload management interfaces, see z/OS MVS Programming: Workload Management Services.

RawCP
The raw WLM server-specific general CP weight.

RawzAAP
The raw WLM server-specific zAAP weight.

RawzIIP
The raw WLM server-specific zIIP weight.

PropCP
The RawCP value modified by the proportion of CP capacity that is currently being consumed by the application's workload as compared to the other processors (zIIP and zAAP).

PropzAAP
The RawzAAP value modified by the proportion of zAAP capacity that is currently being consumed by the application's workload as compared to the other processors (CP and zIIP).

PropzIIP
The RawzIIP value modified by the proportion of zIIP capacity that is currently being consumed by the application's workload as compared to the other processors (CP and zAAP).

ILWeighting
The weighting factor the workload manager (WLM) uses when it

compares displaceable capacity at different importance levels (ILs) in order to determine a SERVERWLM recommendation for each system.

XcostzAAP
The crossover cost that is applied to the workload that was targeted to run on a zAAP processor but that ran on the conventional processor.

XcostzIIP
The crossover cost that is applied to the workload that was targeted to run on a zIIP processor but that ran on the conventional processor.

Application Data
The application data that makes it easy for users to locate and display the connections that are used by the application. The beginning of the application data identifies the format of the application data area. For z/OS Communications Server applications, see application data in the z/OS Communications Server: IP Programmer's Guide and Reference for a description of the format, content, and meaning of the data supplied by the application. For other applications, see the documentation that is supplied by the application. The data is displayed in character format if application data is present. Non-printable characters, if any, are displayed as dots.

- The following fields are displayed for a UDP socket entry:

Client Name
See the Client name or User ID information in Netstat report general concepts for a detailed description.

Client ID
See the Client ID or Connection Number information in Netstat report general concepts for a detailed description.

Local Socket
See the Local Socket information in Netstat report general concepts for a detailed description.

Foreign Socket
See the Foreign Socket information in Netstat report general concepts for a detailed description.

BytesIn
The number of bytes of data the stack has received for this UDP socket. Includes both the total bytes that all applications have received for this socket and the total bytes in stack buffers that have not yet been read by any application.

BytesOut
Number of outbound bytes of user data sent from this socket.

DgramIn
The number of datagrams the stack has received for this UDP socket. This includes both the total datagrams that all applications have received for this socket and the total datagrams in stack buffers that have not yet been read by any application. A datagram is the group of data bytes contained in a UDP packet.

DgramOut
Number of outbound datagrams sent from this socket.

Last touched time
See the Last touched time information in Netstat report general concepts for a detailed description.

MaxSendLim
Maximum allowed size of a user datagram sent from this socket.

MaxRecvLim
Maximum allowed size of a user datagram received on this socket.

SockOpt
Socket option flag. For TCP/IP stacks that are not IPv6 enabled, it is a one-byte hexadecimal value of common socket options. For IPv6-enabled TCP/IP stacks, it is a one-byte hexadecimal value of common socket options, followed by a three-byte hexadecimal value of IPv6-specific socket options.

IPv4 socket options:

80 1... ....
Allow use of broadcast address (IPv4 only)

40 .1.. ....
Allow loopback of datagrams

20 ..1. ....
Bypass normal routing

10 ...1 ....
Forward ICMP messages (Pascal API)

08 .... 1...
Last sent a multicast packet

04 .... .1..
Multicast packets can be received by this socket

02 .... ..1.
Reuse address

other values
reserved

IPv6 socket options:

Byte 1

80 1... ....
AF_INET6 socket

40 .1.. ....
IPV6_V6ONLY option set

20 ..1. ....
IPV6_RECVPKTINFO option set

10 ...1 ....
IPV6_RECVHOPLIMIT option set

08 .... 1...
IPV6_USE_MIN_MTU for unicast option

04 .... .1..
IPV6_PKTINFO src IP@ option set

02 .... ..1.
IPV6_PKTINFO interface index option set

01 1
IPV6_UNICAST_HOPS option set

Byte 2

80 1... ....
IPV6_USE_MIN_MTU for multicast option set

40 .1.. ....
IPV6_RECVRTHDR option set

20 ..1. ....
IPV6_RECVHOPOPTS option set

10 ...1 ....
IPV6_RECVDSTOPTS option set

08 .... 1...
IPV6_RECVTCLASS option set

04 .... .1..
IPV6_NEXTHOP option set

02 .... ..1.
IPV6_RTHDR option set

01 1
IPV6_HOPOPTS option set

Byte 3

80 1... ....
IPV6_DSTOPTS option set

40 .1.. ....
IPV6_RTHDRDSTOPTS option set

20 ..1. ....
IPV6_TCLASS option set

10 ...1 ....
IPV6_DONTFRAG option set

08 .... 1...
IPV6_RECVPATHMTU option set

other values
reserved

DSField
The Differentiated Services Code Point value being used for this connection.

The DSField represents one of the following values:

– If there is a Service Policy Agent policy in effect for this entry, one of the following values is used:
  - The ToS value defined by RFC 791 and 1349
  - The Differentiated Services field value defined by RFC 2474
– For UDP entries for which there is no Service Policy Agent policy in effect but the entry is being used for an Enterprise Extender

connection, the hexadecimal value of one of the following VTAM IP Type of Service values is displayed:

20 Low
40 Medium
80 High
C0 Network

See the z/OS Communications Server: SNA Network Implementation Guide for additional information.

– If neither of these is true, this value is 0.

QOSPolicy
Indicates whether a matching QoS policy rule has been found for this connection. This field can have the following values:

No Indicates that a matching QoS policy rule was not found for this connection.

Yes
Indicates that a matching QoS policy rule was found for this connection. When the QOSPolicy field has the value `Yes`, the following information is displayed:

QOSRuleName
The name of the Policy rule that is in use for this connection. This policy is for outbound traffic only.

RoutingPolicy
Indicates whether a matching routing policy rule has been found for this connection. This field can have the following values:

No Indicates that no matching routing policy rule was found for this connection.

Yes Indicates that a matching routing policy rule was found for this connection.

When the RoutingPolicy field has the value `Yes`, the following information is displayed:

RoutingTableName
The name of the routing table that was used to find the route for this connection or `*NONE*` if a route was not found. The value `EZBMAIN` is displayed when the main routing table was used.

RoutingRuleName
The name of the routing policy rule in use for this connection.

ReceiveDataQueued
The number of bytes of data on the receive queue from the remote application yet to be read. When the number of bytes is not zero, the following information is displayed:

OldQDate
The date of the oldest datagram on the receive queue.

OldQTime
The time of the oldest datagram on the receive queue.

ReceiveMsgCnt
The number of datagrams on the receive queue.

Multicast Specific
Indicates that there is multicast data associated with this socket.

For outgoing multicast data the following field descriptions apply:

HopLimit
The time-to-live value.

LoopBack
Indicates whether datagrams are sent to loopback.

OutgoingIpAddr
The IPv4 IP address of the link on which the datagrams are sent. The value of this field is 0.0.0.0 if the socket has not been set with the IP_MULTICAST_IF setsockopt option. This field is not applicable for an IPv6 multicast entry.

OutgoingIntf
The IPv6 interface name on which the datagrams are sent. The value of this field is blank if the socket has not been set with the IPV6_MULTICAST_IF setsockopt option. This field is not applicable for an IPv4 multicast entry.

For incoming multicast data the following field descriptions apply:

Group The multicast IP addresses (up to a maximum of 20) for which data is being received.

IncomingIpAddr
The IPv4 IP address of the link over which multicast datagrams are accepted. This field is not applicable for an IPv6 multicast entry.

IncomingIntf
The IPv6 interface name over which multicast datagrams are accepted. This field is not applicable for an IPv4 multicast entry.

SrcFltMd
The source filter mode, which can have a value of either `Include` or `Exclude`. A source filter applies only to incoming multicast data. This source filter function is set by an application for the UDP socket. See the information about Designing multicast programs in the z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference for details. The source filter applies to all the IP addresses in the SrcAddr fields for the associated IncomingIPAddr address or IncomingIntf interface.

Include
Indicates that the socket receives only multicast datagrams that have a source IP address that matches an IP address indicated in the SrcAddr field.

Exclude
Indicates either that the source filter function is

not active for the socket or that the application has requested to receive only multicast datagrams that have a source IP address that does not match an IP address indicated in the SrcAddr field. If the source filter function is not active or if the source filter function is active but no SrcAddr value is set, then the SrcAddr field contains the value `None`.

SrcAddr
Source address information for the socket.

ipaddr The source IP addresses (up to a maximum of 64), used in conjunction with the SrcFltMd value, that is used to determine which incoming multicast datagrams should be passed to an application.

None This value is displayed only when the source filter function is not active for the socket or when no source IP address is associated with group multicast address, IncomingIPAddr address, or IncomingIntf interface. The value of the corresponding SrcFltMd field is `Exclude`.

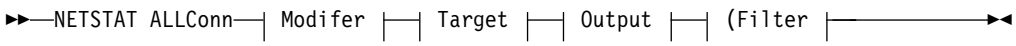
StartDate
See the StartDate information in Netstat report general concepts.

StartTime
See the StartTime information in Netstat report general concepts.

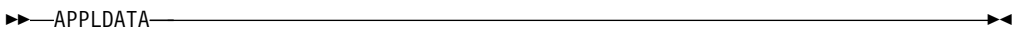
Netstat ALLConn/-a report

Provides information for all TCP connections and UDP sockets, including recently closed ones.

TSO syntax



Modifier



APPLDATA
Provides application data in the output report.

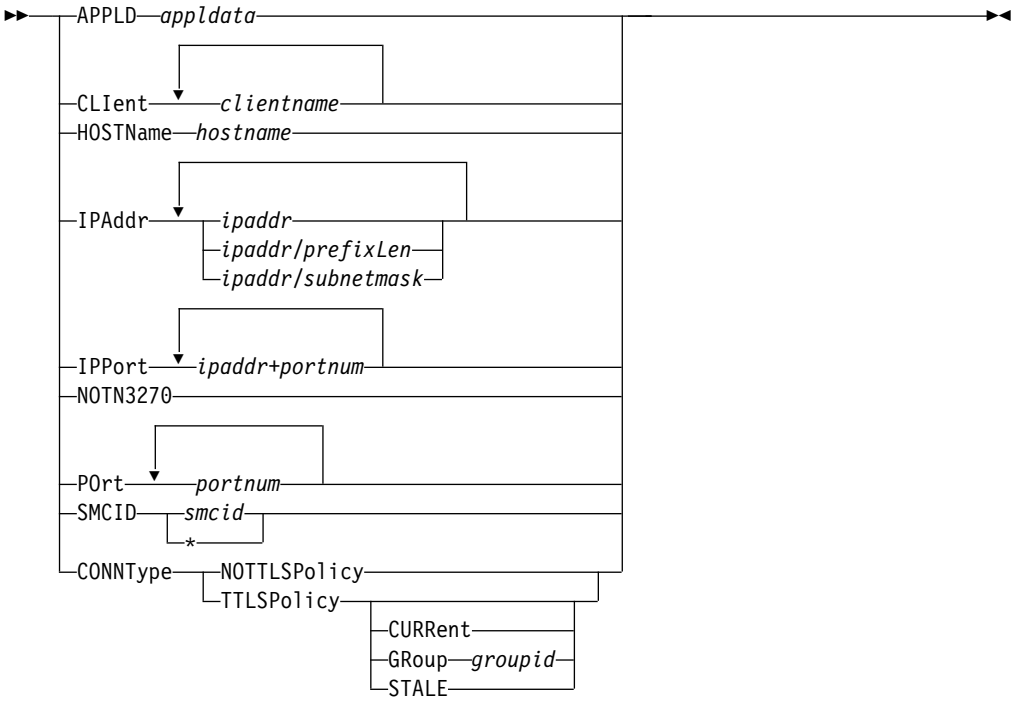
Target

Provide the report for a specified TCP/IP address space by using TCp *tcpname*. See The Netstat command target for more information about the TCp parameter.

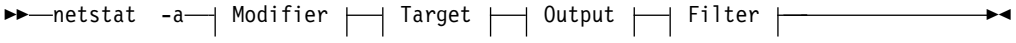
Output

The default output option displays the output on the user's terminal. For other options, see “The TSO NETSTAT command syntax” on page 241 or Netstat command output.

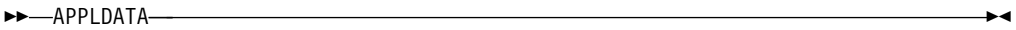
Filter



z/OS UNIX syntax



Modifier



APPLDATA
Provides application data in the output report.

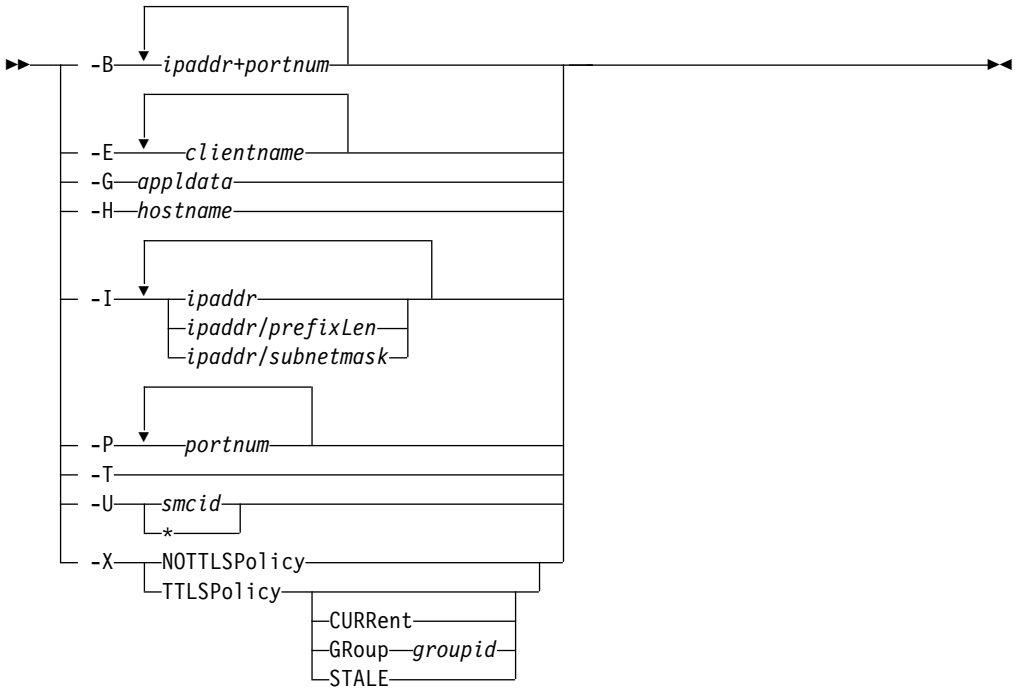
Target

Provide the report for a specified TCP/IP address space by using **-p** *tcpname*. See The Netstat command target for more information about the **-p** parameter.

Output

The default output option displays the output to z/OS UNIX shell stdout. For other options, see "The z/OS UNIX netstat command syntax" on page 245 or Netstat command output.

Filter



Filter description

APPLD/-G *appldata*
Filter the output of the ALLConn/**-a** report using the specified application data *appldata*. You can enter one filter value at a time and the specified value can be up to 40 characters in length.

CLIent/-E *clientname*
Filter the output of the ALLConn/**-a** report using the specified client name *clientname*. You can enter up to six filter values and each specified value can be up to eight characters in length.

HOSTName/-H *hostname*
Filter the output of the ALLConn/**-a** report using the specified host name *hostname*. You can enter one filter value at a time and the specified value can be up to 255 characters in length.

Result: At the end of the report, Netstat displays the host name that the resolver used for the resolution and the list of IP addresses returned from the resolver that it used as filters.

Restrictions:

1. The HOSTName/**-H** filter does not support wildcard characters.
2. Using HOSTName/**-H** filter might cause delays in the output due to resolution of the *hostname* value depending upon resolver and DNS configuration.

IPAddr/-I *ipaddr***IPAddr/-I** *ipaddr/prefixlength***IPAddr/-I** *ipaddr/subnetmask*
Filter the report output using the specified IP address *ipaddr*, *ipaddr/prefixlength*, or *ipaddr/subnetmask*. You can enter up to six filter values. Each specified IPv4 *ipaddr* value can be up to 15 characters in length and each selected IPv6 *ipaddr* value can be up to 45 characters in length.

ipaddr Filter the output of the ALLConn/**-a** report using the specified IP

address *ipaddr*. For IPv4 addresses, the default subnet mask of 255.255.255.255 is used. For IPv6 addresses, the default *prefixlength* of 128 is used.

ipaddr/prefixlength
Filter the output of the ALLConn/**-a** report using the specified IP address and prefix length *ipaddr/prefixlength*. For an IPv4 address, the prefix length range is 1 – 32. For an IPv6 address, the prefix length range is 1 – 128.

ipaddr/subnetmask
Filter the output of the ALLConn/**-a** report using the specified IP address and subnet mask *ipaddr/subnetmask*. The IP address *ipaddr* in this format must be an IPv4 IP address.

Guidelines:

1. The filter value *ipaddr* can be either the local or remote IP address.
2. For an IPv6-enabled stack:
   - Both IPv4 and IPv6 *ipaddr* values are accepted and can be mixed on the IPAddr/**-I** option.
   - An IPv4-mapped IPv6 address is accepted as a valid *ipaddr* value and will usually provide the same result as its IPv4 address.

Restrictions:

1. The filter value for an IPv6 address does not support wildcard characters.
2. For an IPv4-only stack, only IPv4 *ipaddr* values are accepted.
3. For a UDP endpoint socket, the filter value applies only to the local or source IP address.

IPPort/-B *ipaddr+portnum*
Filter the report output of the ALLConn/**-a** report using the specified IP address and port number. You can enter up to six filter values. Each specified IPv4 *ipaddr* value can be up to 15 characters in length, denoting a single IPv4 IP address; each specified IPv6 *ipaddr* value can be up to 45 characters in length, denoting a single IPv6 IP address. Valid *portnum* values are in the range 0 – 65535. The filter values *ipaddr* and *portnum* will match any combination of the local and remote IP address and local and remote port.

Guidelines:

- The filter value *ipaddr* can be either the local or remote IP address.
- For an IPv6-enabled stack, the following apply:
  – Both IPv4 and IPv6 *ipaddr* values are accepted and can be mixed on the IPPort/**-B** option.
  – An IPv4-mapped IPv6 address is accepted as a valid *ipaddr* value and usually provides the same result as the IPv4 address.

Restrictions:

- The *ipaddr* value in the IPPort/**-B** filter does not support wildcard characters.
- For an IPv4-only stack, only IPv4 *ipaddr* values are accepted.
- An entry is returned only when both the *ipaddr* and *portnum* values match.

- For a UDP endpoint socket, the filter value applies only to the local or source IP address and port.

NOTN3270/-T
Filter the output of the ALLConn/**-a** report, excluding TN3270 server connections.

POrt/-P *portnum*
Filter the output of the ALLConn/**-a** report using the specified port number *portnum*. You can enter up to six filter values.

Guideline: The port number can be either a local or remote port.

Restriction: For a UDP endpoint socket, the filter value applies only to the local or source port.

SMCID/-U *smcid*
Filter the output of the ALLConn/-a report by using the specified Shared Memory Communications over Remote Direct Memory Access (SMC-R) link, SMC-R link group, or Shared Memory Communications - Direct Memory Access (SMC-D) link identifier *smcid*. If an asterisk (*) is specified for the filter value, Netstat provides output only for entries that are associated with SMC-R links, SMC-R link groups, and SMC-D links. You can enter one filter value at a time.

CONNType/-X
Filter the report using the specified connection type. You can enter one filter value at a time.

NOTTLSPolicy
Filter the output of the ALLConn/**-a** report, displaying only connections that have not been matched to an Application Transparent Transport Layer Security (AT-TLS) rule. This includes connections that were established while the AT-TLS function was disabled (the value NOTTLS was specified on the TCPCONFIG statement or is in effect by default) and all connections that are not TCP protocol. For TCP connections that were established while the AT-TLS function was enabled, this includes the following information:

- Connections for which AT-TLS policy lookup has not yet occurred (typically the first send or receive has not been issued yet)
- Connections for which AT-TLS policy lookup has occurred but no matching rule was found

TTLSPolicy
Filter the output of the ALLConn/**-a** report, displaying only connections that match an Application Transparent Transport Layer Security (AT-TLS) rule. This includes only connections that were established while the AT-TLS function was enabled, for which an AT-TLS policy rule was found that has the value `TTLSEnabled ON` or `TTLSEnabled OFF` specified in the TTLSGroupAction policy statement. Responses can be further limited on AT-TLS connection type. AT-TLS connection type has the following values:

CURRent
Display only connections that are using AT-TLS where the rule and all actions are still available to be used for new connections.

GRoup *groupid*
Display only connections that are using the AT-TLS group specified by the *groupid* value. The specified *groupid* value is a number that is assigned by the TCP/IP stack to uniquely identify an AT-TLS group. You can determine the *groupid* value from the GroupID field in the Netstat TTLS/**-x** GROUP report.

STALE
Display only connections that are using AT-TLS where the rule or at least one action is no longer available to be used for new connections.

The filter value for CLIent/**-E**, IPAddr/**-I**, and APPLD/-G can be a complete string or a partial string using wildcard characters. A wildcard character can be an asterisk (*), which matches a null string or any character or character string, at the same position. A wildcard character can be a question mark (?), which matches any single character at the same position. For example, a string *searchee* matches with **ar?he**, but the string *searhee* does not match with **ar?he**. If you want to use the wildcard character on the IPAddr/**-I** filter, you must specify the value in the *ipaddr* format. The wildcard character is not accepted for the *ipaddr/prefixlen* or *ipaddr/subnetmask* format of IPAddr/**-I** values.

When you use z/OS UNIX **netstat**/**onetstat** command in a z/OS UNIX shell environment, take care if you use a z/OS UNIX MVS special character in a character string. It might cause an unpredictable result. To be safe, if you want to use a z/OS UNIX MVS special character in a character string, surround the character string with single quotation marks. For example, to use an asterisk (*) in the IP address, 10.*.0.0 for the **-I** filter, issue the command as: **netstat -a -I '10.*.0.0'**.

Command syntax examples

From TSO environment

```
NETSTAT ALLCONN
   Display information for all TCP connections and UDP sockets, including recently closed
   ones in the default TCP/IP stack.
NETSTAT ALLCONN TCP TCPCS6
   Display information for all TCP connections and UDP sockets, including recently closed
   ones in TCPCS6 stack.
NETSTAT ALLCONN TCP TCPCS8 (IPADDR 9.43.1.1 9.43.2.2
   Display information for these TCP connections and UDP sockets, including recently closed
   ones in TCPCS8 stack whose local or remote IP addresses match the specified filter IP
   address values.
NETSTAT ALLCONN (PORT 2222 6666 88
   Display information for those TCP connections and UDP sockets, including recently closed
   ones in the default TCP/IP stack whose local or remote ports match the specified filter
   port numbers.
```

From UNIX shell environment

```
   netstat -a
   netstat -a -p tcpcs6
   netstat -a -p tcpcs6 -I 9.43.1.1 9.43.2.2
   netstat -a -P 2222 6666 88
```

Report examples

The following examples are generated using the TSO NETSTAT command. The z/OS UNIX **netstat** command displays the data in the same format as the TSO NETSTAT command.

Not IPv6 enabled (SHORT format)

```
NETSTAT ALLCONN
MVS TCP/IP NETSTAT CS V2R3       TCPIP NAME: TCPCS            17:40:36
User Id  Conn     Local Socket           Foreign Socket         State
-------  ----     ------------           --------------         -----
FTPD1    0000003B 0.0.0.0..21            0.0.0.0..0             Listen
FTPD1    0000003D 9.37.65.146..21        9.67.115.5..1026       Establsh
FTPD1    0000003F 9.37.65.146..21        9.27.13.21..3711       Establsh
TCPCS    0000000F 0.0.0.0..23            0.0.0.0..0             Listen
TCPCS    0000000C 9.67.115.5..23         9.27.11.182..4886      Establsh
USER1    00000027 9.67.115.67..1027      9.67.115.5..21         ClosWait
USER1    00000029 9.67.115.69..1028      9.67.115.5..20         ClosWait
APPV4    00000015 0.0.0.0..2049          9.42.103.99..1234      UDP
SYSLOGD1 00000010 0.0.0.0..514           *..*                   UDP
```

IPv6 enabled or request for LONG format

```
NETSTAT ALLCONN
MVS TCP/IP NETSTAT CS V2R3       TCPIP NAME: TCPCS            17:40:36
User Id  Conn     State
-------  ----     -----
FTPD1    0000004A Listen
  Local Socket:   ::..21
  Foreign Socket: ::..0
FTPD1    00000052 Establsh
  Local Socket:   ::ffff:9.67.115.5..21
  Foreign Socket: ::ffff:9.67.115.65..1026
FTPD1    00000058 Establsh
  Local Socket:   2001:0db8::9:67:115:66..21
  Foreign Socket: 2001:0db8::9:67:115:65..1027
TCPCS    0000001A Listen
  Local Socket:   0.0.0.0..23
  Foreign Socket: 0.0.0.0..0
TCPCS    0000001E Establsh
  Local Socket:   9.67.115.5..23
  Foreign Socket: 9.27.11.182..4665
USER3    0000005F Establsh
  Local Socket:   2001:0db8::9:67:115:5..1079
  Foreign Socket: 2001:0db8::9:67:115:65..21
USER6    000000C7 Establsh
  Local Socket:   9.67.115.5..1027
  Foreign Socket: 9.37.65.146..21
USER8    000000B7 ClosWait
  Local Socket:   9.67.115.5..1027
  Foreign Socket: 9.37.65.146..21
USER8    000000B8 FinWait2
  Local Socket:   2001:0db8::9:67:115:5..21
  Foreign Socket: 2001:0db8::9:67:115:65..1083
APPM     00000017 UDP
  Local Socket:   ::ffff.0.0.0.0..2051
  Foreign Socket: ::ffff.9.42.103.99..1236
APPV4    00000015 UDP
  Local Socket:   0.0.0.0..2049
  Foreign Socket: 9.42.103.99..1234

SYSLOGD1 0000002C UDP
  Local Socket:   0.0.0.0..529
  Foreign Socket: *..*
```

Report field descriptions

User Id
See the Client name or User ID information in Netstat report general concepts for a detailed description.

Conn See the Client ID or Connection Number information in Netstat report general concepts for a detailed description.

Local Socket
See the Local Socket information in Netstat report general concepts for a detailed description.

Foreign Socket
See the Foreign Socket information in Netstat report general concepts for a detailed description.

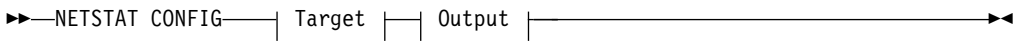
State See the TCP connection status and UDP socket status information in Netstat report general concepts for a detailed description.

Application Data
The application data that makes it easy for users to locate and display the connections that are used by the application. The beginning of the application data identifies the format of the application data area. For z/OS Communications Server applications, see application data information in the z/OS Communications Server: IP Programmer's Guide and Reference for a description of the format, content, and meaning of the data supplied by the application. For other applications, see the documentation that is supplied by the application. The data is displayed in character format if application data is present. Non-printable characters, if any, are displayed as dots.

Netstat CONFIG/-f report

Displays TCP/IP configuration information about IP, TCP, UDP, SMF parameters, GLOBALCONFIG profile statement, network monitor, data trace, and autolog settings.

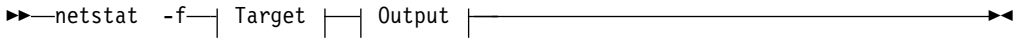
TSO syntax



Target
Provide the report for a specific TCP/IP address space by using the TCp *tcpname* parameter. See The Netstat command target for more information about the TCp parameter.

Output
The default output option displays the output on the user's terminal. For other options, see “The TSO NETSTAT command syntax” on page 241 or Netstat command output.

z/OS UNIX syntax



Target

Provide the report for a specific TCP/IP address space by using the **-p** *tcpname* option. See The Netstat command target for more information about the TCp parameter.

Output

The default output option displays the output to z/OS UNIX shell stdout. For other options, see "The z/OS UNIX netstat command syntax" on page 245 or Netstat command output.

Command syntax examples

From TSO environment

```
NETSTAT CONFIG
Display the TCP/IP configuration information for the default TCP/IP stack.
NETSTAT CONFIG TCP TCPCS6
Display the TCP/IP configuration information for TCPCS6 stack.
```

From UNIX shell environment

```
   netstat -f
   netstat -f -p tcpcs6
```

Report examples

The following examples are generated by using TSO NETSTAT command. Using the z/OS UNIX **netstat** command displays the data in the same format as the TSO NETSTAT command.

Not IPv6 enabled (SHORT format)

```
NETSTAT CONFIG MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           11:37:31
TCP Configuration Table:
DefaultRcvBufSize:  00016384  DefaultSndBufSize: 00016384
DefltMaxRcvBufSize: 00262144  SoMaxConn:         0000001024
MaxReTransmitTime:  120.000   MinReTransmitTime: 0.500
RoundTripGain:      0.125     VarianceGain:      0.250
VarianceMultiplier: 2.000     MaxSegLifeTime:    30.000
DefaultKeepALive:   00000120  DelayAck:          Yes
RestrictLowPort:    Yes       SendGarbage:       No
TcpTimeStamp:       Yes       FinWait2Time:      010
TTLS:               No        EphemeralPorts:    1024-65535
SelectiveACK:       Yes       TimeWaitInterval:  30
DefltMaxSndBufSize  262144    RetransmitAttempt: 15
ConnectTimeOut:     0120      ConnectInitIntval: 1000
KeepAliveProbes:    10        KAProbeInterval:   060
Nagle:              No        QueuedRTT:         20
FRRThreshold:       3

UDP Configuration Table:
DefaultRcvBufSize: 00065535  DefaultSndBufSize: 00065535
CheckSum:          Yes       EphemeralPorts:    1024-65535
RestrictLowPort:   Yes       UdpQueueLimit:     No

IP Configuration Table:
Forwarding: Yes    TimeToLive: 00064  RsmTimeOut:  00060
IpSecurity: Yes
ArpTimeout: 01200  MaxRsmSize: 65535  Format:      Short
IgRedirect: Yes    SysplxRout: No     DoubleNop:   No
StopClawEr: No     SourceVipa: Yes
MultiPath:  Conn   PathMtuDsc: No     DevRtryDur:  0000000090
DynamicXCF: Yes
  IpAddr/PrefixLen: 193.9.200.3/28      Metric: 01
  SecClass: 008  SrcVipaInt: IPV4SRCVIPA
  SMCD:     Yes
QDIOAccel:  No
IQDIORoute: No
TcpStackSrcVipa: 201.1.10.10
ChecksumOffload: Yes             SegOffload: Yes

SMF Parameters:
Type 118:
  TcpInit:      00   TcpTerm:      02   FTPClient:    03
  TN3270Client: 04   TcpIpStats:   05
Type 119:
  TcpInit:      Yes  TcpTerm:      Yes  FTPClient:    Yes
  TcpIpStats:   Yes  IfStats:      Yes  PortStats:    Yes
  Stack:        Yes  UdpTerm:      Yes  TN3270Client: Yes
  IPSecurity:   No   Profile:      Yes  DVIPA:        Yes
  SmcrGrpStats: Yes  SmcrLnkEvent: Yes
```

```
Global Configuration Information:
TcpIpStats: Yes  ECSALimit: 2096128K  PoolLimit: 2096128K
MlsChkTerm: No   XCFGRPID:  11        IQDVLANID: 27
SysplexWLMPoll: 060  MaxRecs:   100
ExplicitBindPortRange:  05000-06023   IQDMultiWrite: Yes
AutoIQDX: AllTraffic                  AdjustDVIPAMSS: Auto
WLMPriorityQ: Yes
  IOPri1 0 1
  IOPri2 2
  IOPri3 3 4
  IOPri4 5 6 FWD
Sysplex Monitor:
  TimerSecs: 0060  Recovery: Yes  DelayJoin: No   AutoRejoin: Yes
  MonIntf:   Yes   DynRoute: Yes  Join:      Yes
zIIP:
  IPSecurity: Yes  IQDIOMultiWrite: Yes
SMCGlobal:
  AutoCache:  Yes  AutoSMC: Yes
SMCR: Yes
  FixedMemory: 100M  TcpKeepMinInt: 00000300
  PFID: 0018  PortNum: 1 MTU: 1024
  PFID: 0019  PortNum: 2 MTU: 1024
SMCD: Yes
  FixedMemory: 100M  TcpKeepMinInt: 00000300
```

```
Network Monitor Configuration Information:
PktTrcSrv: Yes  TcpCnnSrv: Yes  MinLifTim: 3  NtaSrv: Yes
SmfSrv: Yes
  IPSecurity: Yes  Profile: Yes  CSSMTP: Yes  CSMAIL: Yes  DVIPA: Yes

Autolog Configuration Information: Wait Time: 0300
ProcName: FTPD      JobName: FTPD
  ParmString:
  DelayStart: Yes
    DVIPA    TTLS
```

IPv6 enabled or request for LONG format

```
NETSTAT CONFIG
MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           19:54:08
TCP Configuration Table:
DefaultRcvBufSize:  00016384  DefaultSndBufSize: 00016384
DefltMaxRcvBufSize: 00262144  SoMaxConn:         0000001024
MaxReTransmitTime:  120.000   MinReTransmitTime: 0.500
RoundTripGain:      0.125     VarianceGain:      0.250
VarianceMultiplier: 2.000     MaxSegLifeTime:    30.000
DefaultKeepALive:   00000120  DelayAck:          Yes
RestrictLowPort:    Yes       SendGarbage:       No
TcpTimeStamp:       Yes       FinWait2Time:      010
TTLS:               No        EphemeralPorts:    1024-65535
SelectiveACK:       Yes       TimeWaitInterval:  30
DefltMaxSndBufSize  262144    RetransmitAttempt: 15
ConnectTimeOut:     0120      ConnectInitIntval: 1000
KeepAliveProbes:    10        KAProbeInterval:   060
Nagle:              No        QueuedRTT:         20
FRRThreshold:       3

UDP Configuration Table:
DefaultRcvBufSize: 00065535  DefaultSndBufSize: 00065535
CheckSum:          Yes       EphemeralPorts:    1024-65535
RestrictLowPort:   Yes       UdpQueueLimit:     No

IP Configuration Table:
Forwarding: Yes    TimeToLive: 00064  RsmTimeOut:  00060
IpSecurity: Yes
ArpTimeout: 01200  MaxRsmSize: 65535  Format:      Long
IgRedirect: Yes    SysplxRout: No     DoubleNop:   No
StopClawEr: No     SourceVipa: Yes
MultiPath:  Conn   PathMtuDsc: No     DevRtryDur:  0000000090
DynamicXCF: Yes
  IpAddr/PrefixLen: 193.9.200.3/28      Metric: 01
  SecClass: 008  SrcVipaInt: IPV4SRCVIPA
QDIOAccel:  Yes       QDIOAccelPriority: 2
IQDIORoute: n/a
TcpStackSrcVipa: 201.1.10.10
ChecksumOffload: Yes             SegOffload: Yes

IPv6 Configuration Table:
Forwarding:    Yes  HopLimit:   00255  IgRedirect:  No
SourceVipa:    Yes  MultiPath:  Conn   IcmperrLim:  00003
IgRtrHopLimit: No
IpSecurity: Yes
  OSMSecClass: 255
DynamicXCF: Yes
  IpAddr: 2001:db8::9:67:115:5
  IntfID: 0009:0067:0011:0001
  SrcVipaInt: IPV6SRCVIPA
  SecClass: 008
TcpStackSrcVipa: IPV6STKSRCVIPA
TempAddresses: Yes
  PreferredLifetime: 24   ValidLifetime: 168
ChecksumOffload: Yes             SegOffload: Yes

SMF Parameters:
Type 118:
  TcpInit:      00   TcpTerm:      02   FTPClient:    03
  TN3270Client: 04   TcpIpStats:   05
Type 119:
  TcpInit:      Yes  TcpTerm:      Yes  FTPClient:    Yes
  TcpIpStats:   Yes  IfStats:      Yes  PortStats:    Yes
  Stack:        Yes  UdpTerm:      Yes  TN3270Client: Yes
  IPSecurity:   No   Profile:      Yes  DVIPA:        Yes
  SmcrGrpStats: Yes  SmcrLnkEvent: Yes
```

```
Global Configuration Information:
TcpIpStats: Yes  ECSALimit: 2096128K  PoolLimit: 2096128K
MlsChkTerm: No   XCFGRPID:  11        IQDVLANID: 27
SysplexWLMPoll: 060  MaxRecs:   100
ExplicitBindPortRange:  05000-06023   IQDMultiWrite: Yes
AutoIQDX: AllTraffic
WLMPriorityQ: Yes
  IOPri1 0 1
  IOPri2 2
  IOPri3 3 4
  IOPri4 5 6 FWD
Sysplex Monitor:
  TimerSecs: 0060  Recovery: Yes  DelayJoin: No   AutoRejoin: Yes
  MonIntf:   Yes   DynRoute: Yes  Join:      Yes
zIIP:
  IPSecurity: Yes  IQDIOMultiWrite: Yes
SMCR: Yes
  FixedMemory: 100M  TcpKeepMinInt: 00000300
  PFID: 0018  PortNum: 1 MTU: 1024
  PFID: 0019  PortNum: 2 MTU: 1024

Network Monitor Configuration Information:
PktTrcSrv: Yes  TcpCnnSrv: Yes  MinLifTim: 3  NtaSrv: Yes
SmfSrv:    Yes
  IPSecurity: Yes  Profile: Yes  CSSMTP: Yes  CSMAIL: Yes  DVIPA: Yes

Data Trace Setting:
JobName: *         TrRecCnt: 00000000  Length: FULL
IpAddr:  *                 SubNet: *
PortNum: *

Autolog Configuration Information: Wait Time: 0300
ProcName: FTPD      JobName: FTPD
  ParmString:
  DelayStart: Yes
    DVIPA    TTLS
```

Report field descriptions

- **TCP Configuration Table**

  Display the following configured TCP information that is defined in the TCPCONFIG and SOMAXCONN profile statements. For more information about each field, see the TCPCONFIG or SOMAXCONN profile statement information in z/OS Communications Server: IP Configuration Reference.

  DefaultRcvBufSize
  The TCP receive buffer size that was defined using the TCPRCVBUFRSIZE parameter in the TCPCONFIG statement. The size is between 256 and TCPMAXRCVBUFRSIZE; the default size is 65536 (64 KB). This value is used as the default receive buffer size for those applications that do not explicitly set the buffer size using SETSOCKOPT(). If the TCPRCVBUFRSIZE parameter was not specified in the TCPCONFIG statement, then the default size 65536 (64 KB) is displayed.

  DefaultSndBufSize
  The TCP send buffer size that was defined using the TCPSENDBFRSIZE parameter in the TCPCONFIG statement. The size is between 256 bytes and TCPMAXSENDBUFRSIZE; the default size is 65536 (64 KB). This value is used as the default send buffer size for those applications that do not explicitly set the buffer size using SETSOCKOPT(). If the TCPSENDBFRSIZE parameter was not specified in the TCPCONFIG statement, then the default size 65536 (64 KB) is displayed.

  DefltMaxRcvBufSize
  The TCP maximum receive buffer size that was defined using the TCPMAXRCVBUFRSIZE parameter in the TCPCONFIG statement. The

maximum receive buffer size is the maximum value that an application can set as its receive buffer size using SETSOCKOPT(). The minimum acceptable value is the value that is coded on the TCPRCVBUFRSIZE parameter, the maximum size is 2 MB, and the default size is 256 KB. If you do not have large bandwidth interfaces, you can use this parameter to limit the receive buffer size that an application can set. If the TCPMAXRCVBUFRSIZE parameter was not specified in the TCPCONFIG statement, then the default size 262144 (256 KB) is displayed.

SoMaxConn
The maximum number of connection requests that can be queued for any listening socket, as defined by the SOMAXCONN statement. The minimum value is 1, the maximum value is 2147483647, and the default value is 1024.

MaxReTransmitTime
The maximum retransmit interval in seconds. The range is 0 - 999.990. The default value is 120.

Rules:

– If none of the following parameters is specified, this MAXIMUMRETRANSMITTIME parameter is used and the MINIMUMRETRANSMITTIME parameters of the following statements are not used.
  - MAXIMUMRETRANSMITTIME on the BEGINROUTES statement
  - MAXIMUMRETRANSMITTIME on the GATEWAY statement
  - MAXIMUMRETRANSMITTIME on the ROUTETABLE statement
  - Max_Xmit_Time on the OSPF_INTERFACE statement
  - Max_Xmit_Time on the RIP_INTERFACE statement
– The TCPCONFIG version is used if no route parameter has been explicitly specified. If the TCPCONFIG version of maximum retransmit time is used, the MINIMUMRETRANSMITTIME value that is specified on the route parameter is not used, which means the value of the minimum retransmit time is 0.

DefaultKeepAlive
The default keepalive interval that was defined using the INTERVAL parameter in the TCPCONFIG statement. It is the number of minutes that TCP waits after it receives a packet for a connection before it sends a keepalive packet for that connection. The range is 0 - 35791 minutes; the default value is 120. The value 0 disables the keepalive function. If the INTERVAL parameter was not specified in the TCPCONFIG statement, then the default interval 120 is displayed.

DelayAck
Indicates whether the DELAYACKS option is enabled or disabled. The value `Yes` indicates that acknowledgments are delayed when a packet is received (the DELAYACKS parameter was defined in the TCPCONFIG profile statement or is in effect by default); the value `No` indicates that acknowledgments are not delayed when a packet is received (the NODELAYACKS parameter was defined in the TCPCONFIG statement).

RestrictLowPort
Indicates whether ports in the range 1 - 1023 are reserved for users by the PORT and PORTRANGE statements. The value `Yes` indicates that RESTRICTLOWPORTS is in effect (the RESTRICTLOWPORTS parameter

was defined in the TCPCONFIG profile statement); the value `No` indicates that RESTRICTLOWPORTS is not in effect (the UNRESTRICTLOWPORTS parameter was defined in the TCPCONFIG statement or is in effect by default).

SendGarbage
Indicates whether the keepalive packets sent by TCP contain 1 byte of random data. The value `Yes` indicates that SENDGARBAGE TRUE is in effect (SENDGARBAGE TRUE was defined in the TCPCONFIG profile statement); the value `No` indicates that SENDGARBAGE TRUE is not in effect (SENDGARBAGE FALSE was defined in the TCPCONFIG statement or is in effect by default).

TcpTimeStamp
Indicates whether the TCP Timestamp Option is enabled or disabled. The value `Yes` indicates that TCPTIMESTAMP is in effect (the TCPTIMESTAMP parameter was defined in the TCPCONFIG profile statement or is in effect by default); the value `No` indicates that TCPTIMESTAMP is not in effect (the NOTCPTIMESTAMP parameter was defined in the TCPCONFIG statement).

FinWait2Time
The FinWait2Time number that was defined using the FINWAIT2TIME parameter in the TCPCONFIG statement. It is the number of seconds a TCP connection should remain in the FINWAIT2 state. The range is 60 - 3600 seconds; the default value is 600 seconds. When this timer expires, it is reset to 75 seconds; when this timer expires a second time, the connection is dropped. If the FINWAIT2TIME parameter was not specified in the TCPCONFIG statement, then the default value 600 is displayed.

TimeWaitInterval
The number of seconds that a connection remains in TIMEWAIT state. The range is 0 - 120. The default value is 60.

Note: For local connections, a TIMEWAITINTERVAL of 50 milliseconds is always used.

DefltMaxSndBufSize
The maximum send buffer size. The range is the value that is specified on TCPSENDBFRSIZE to 2 MB. The default value is 256K.

RetransmitAttempt
The number of times a segment is retransmitted before the connection is aborted. The range is 0 - 15. The default value is 15.

ConnectTimeOut
The total amount of time before the initial connection times out. This value also applies to TCP connections that are established over SMC-R links. The range is 5 - 190 seconds. The default value is 75.

ConnectInitIntval
The initial retransmission interval for the connect(). The range is 100 to 3000 milliseconds (ms). The default value is 3000.

KAProbeInterval
The interval in seconds between keepalive probes. The range is 1 - 75. The default value is 75.

This parameter does not change the initial keepalive timeout interval. It controls the time between the probes that are sent only after the initial keepalive interval has expired.

You can specify setsockopt() TCP_KEEPALIVE to override the parameter.

KeepAliveProbes
The number of keepalive probes to send before the connection is aborted. The range is 1 - 10. The default value is 10.

This parameter does not change the initial keepalive timeout interval. It controls the number of probes that are sent only after the initial keepalive interval has expired.

You can specify setsockopt() TCP_KEEPALIVE to override this parameter.

Nagle Indicates whether the Nagle option is enabled or disabled. The value Yes indicates that packets with less than a full maximum segment size (MSS) of data are buffered unless all data on the send queue has been acknowledged.

QueuedRTT
The threshold at which outbound serialization is engaged. The range is 0 - 50 milliseconds. The default value is 20 milliseconds.

FRRTheshold
The threshold of duplicate ACKs for FRR to engage. The range is 1 - 2048. The default value is 3.

TTLS Indicates whether Application Transparent Transport Layer Security (AT-TLS) is active in the TCP/IP stack. The value `Yes` indicates that AT-TLS is active (the TTLS parameter was specified in the TCPCONFIG profile statement). The value `No` indicates that AT-TLS is not active (the NOTTLS parameter was specified in the TCPCONFIG profile statement or is in effect by default).

EphemeralPorts
The range of ephemeral ports that was defined using the EPHEMERALPORTS parameter in the TCPCONFIG statement or by default. The range specified must be within the range of 1024 to 65535. If the EPHEMERALPORTS parameter was not specified in the TCPCONFIG statement, then the default range 1024 - 65535 is displayed.

SelectiveACK
Indicates whether Selective Acknowledgment (SACK) support is active in the TCP/IP stack. This field can have the following values:

Yes Indicates that SACK options are exchanged with partners when transmitting data. The SELECTIVEACK parameter was specified on the TCPCONFIG profile statement.

No Indicates that SACK options will not be exchanged. The NOSELECTIVEACK parameter was specified on the TCPCONFIG profile statement or is in effect by default.

Note: The values displayed in the MaxReTransmitTime, MinReTransmitTime, RoundTripGain, VarianceGain, VarianceMultiplier, and MaxSegLifeTime fields are actual default values that are assigned by the TCP/IP stack; you cannot configure them externally using the TCPCONFIG profile statement. You can override the MaxReTransmitTime, MinReTransmitTime, RoundTripGain, VarianceGain, VarianceMultiplier values on a per-destination basis using either

the BEGINROUTES configuration statement, the old GATEWAY configuration statement, or the configuration file for OMPROUTE.

- **UDP Configuration Table**

  Display the following configured UDP information defined in the UDPCONFIG profile statement. For more information about each UDP parameter, see UDPCONFIG profile statement information in the z/OS Communications Server: IP Configuration Reference.

  DefaultRcvBufSize
  The UDP receive buffer size that was defined using the UDPRCVBUFRSIZE parameter in the UDPCONFIG statement. The size is in the range 1 - 65535; the default size is 65535. If the UDPRCVBUFRSIZE parameter was not specified in the UDPCONFIG statement, then the default size 65535 is displayed.

  DefaultSndBufSize
  The UDP send buffer size that was defined using the UDPSENDBFRSIZE parameter in the UDPCONFIG statement. The size is in the range 1 - 65535; the default size is 65535. If the UDPSENDBFRSIZE parameter was not specified in the UDPCONFIG statement, then the default size 65535 is displayed.

  CheckSum
  Indicates whether UDP does check summing. The value `Yes` indicates that UDP check summing is in effect (the UDPCHKSUM parameter was defined in the UDPCONFIG profile statement or is in effect by default); the value `No` indicates that UDP check summing is not in effect (the NOUDPCHKSUM parameter was defined in the UDPCONFIG statement).

  EphemeralPorts
  The range of ephemeral ports that was defined using the EPHEMERALPORTS parameter in the UDPCONFIG statement or by default. The range specified must be within the range of 1024 to 65535. If the EPHEMERALPORTS parameter was not specified in the UDPCONFIG statement, then the default range 1024 - 65535 is displayed.

  RestrictLowPort
  Indicates whether ports 1 - 1023 are reserved for users by the PORT and PORTRANGE statements. The value `Yes` indicates that ports in the range 1 - 1023 are reserved (the RESTRICTLOWPORTS parameter was defined in the UDPCONFIG profile statement); the value `No` indicates that the ports are not reserved (the UNRESTRICTLOWPORTS parameter was defined in the UDPCONFIG statement or is in effect by default).

  UdpQueueLimit
  Indicates whether UDP should have a queue limit on incoming datagrams. The value `Yes` indicates that there is a UDP queue limit in effect (the UDPQUEUELIMIT parameter was defined in the UDPCONFIG profile statement or is in effect by default); the value `No` indicates that a UDP queue limit is not in effect (the NOUDPQUEUELIMIT parameter was defined in the UDPCONFIG statement).

- **IP Configuration Table**

Displays the following configured IP information defined in the IPCONFIG profile statement. For more information about each IP parameter, see the IPCONFIG profile statement information in the z/OS Communications Server: IP Configuration Reference.

Forwarding
Indicates whether the transfer of data between networks is enabled for this TCP/IP stack. Possible values are:

Pkt Indicates that packets that are received but not destined for this stack are forwarded and use multipath routes if they are available on a per-packet basis (the DATAGRAMFWD FWDMULTIPATH PERPACKET was specified in the IPCONFIG profile statement).

Yes Indicates that packets that are received but not destined for this stack are forwarded but do not use multipath routes even if they are available. (the DATAGRAMFWD NOFWDMULTIPATH was specified in the IPCONFIG profile statement or is in effect by default).

No Indicates that packets that are received but that are not destined for this stack are not forwarded in route to the destination (the NODATAGRAMFWD parameter was specified in the IPCONFIG profile statement).

TimeToLive
The time to live value that was defined using the TTL parameter in the IPCONFIG statement. The time to live value is the number of hops that packets originating from this host can travel before reaching the destination. Valid values are in the range 1 - 255; the default value is 64. If the TTL parameter was not specified in the IPCONFIG statement, then the default value 64 is displayed.

RsmTimeOut
The reassembly timeout value that was defined using the REASSEMBLYTIMEOUT parameter in the IPCONFIG statement. It is the amount of time (in seconds) that is allowed to receive all parts of a fragmented packet before discarding the packets received. Valid values are in the range 1 - 240; the default value is 60. If the REASSEMBLYTIMEOUT parameter was not specified in the IPCONFIG statement, then the default value 60 is displayed.

IpSecurity
Indicates whether the IP filtering and IPSec tunnel support is enabled. The value `Yes` indicates that IP security is in effect (the IPSECURITY parameter was defined on the IPCONFIG profile statement). The value `No` indicates that IP security is not in effect.

ArpTimeout
The ARP timeout value that was defined using the ARPTO parameter in the IPCONFIG statement. It indicates the number of seconds between creation or revalidation and deletion of ARP table entries. Valid values are in the range 60 - 86400; the default value is 1200. If the ARPTO parameter was not specified in the IPCONFIG statement, then the default value 1200 is displayed.

MaxRsmSize
The maximum packet size that can be reassembled. If an IP datagram is

fragmented into smaller packets, the complete reassembled datagram cannot exceed this value. Valid values are in the range 576 - 65535; the default value is 65535.

Restriction: The value that is displayed in the MaxRsmSize field is the actual default value that was assigned by the TCP/IP stack; users cannot configure this value externally using the IPCONFIG profile statement.

Format
The stack-wide command format that was defined using the FORMAT parameter in the IPCONFIG statement or that was assigned by default by TCP/IP stack. This field can have the following values:

SHORT
Indicates that the command report is displayed in the short format (the FORMAT SHORT parameter was specified in the IPCONFIG profile statement).

LONG
Indicates that the command report is displayed in the long format (the FORMAT LONG parameter was specified in the IPCONFIG profile statement).

If the FORMAT parameter was not specified in the IPCONFIG profile statement, then the TCP/IP stack assigned the default format based on whether the stack was IPv6 enabled or not. If the stack is IPv6 enabled, then the format value LONG is assigned by default. If the stack is configured for IPv4-only operation, then the format value SHORT is assigned by default. You can override the stack-wide command format using the Netstat FORMAT/**-M** option.

IgRedirect
Indicates whether TCP/IP is to ignore ICMP Redirect packets. This field can have the following values:

Yes Indicates that IGNOREREDIRECT is in effect. The IGNOREREDIRECT parameter was defined on the IPCONFIG profile statement, OMPROUTE has been started and IPv4 interfaces are configured to OMPROUTE, or intrusion detection services (IDS) policy is in effect to detect and discard ICMP Redirects.

No Indicates that ICMP Redirects are not ignored.

SysplxRout
Indicates whether this TCP/IP host is part of an MVS sysplex domain and should communicate interface changes to the workload manager (WLM). This field can have the following values:

Yes Indicates that SYSPLEXROUTING is in effect (the SYSPLEXROUTING parameter was specified in the IPCONFIG profile statement).

No Indicates that SYSPLEXROUTING is not in effect (the NOSYSPLEXROUTING parameter was specified in the IPCONFIG profile statement or is in effect by default).

DoubleNop
Indicates whether to force channel programs for CLAW devices to have two NOP CCWs to end the channel programs. This field can have the following values:

Yes Indicates that CLAWUSEDOUBLENOP is in effect (the CLAWUSEDOUBLENOP parameter was defined on the IPCONFIG profile statement).

No Indicates that CLAWUSEDOUBLENOP is not in effect.

StopClawEr
Indicates whether to stop channel programs (HALTIO and HALTSIO) when a device error is detected. This field can have the following values:

Yes Indicates that STOPONCLAWERROR is in effect (the STOPONCLAWERROR parameter was specified in the IPCONFIG profile statement).

No Indicates that STOPONCLAWERROR is not in effect.

SourceVipa
Indicates whether the TCP/IP stack uses the corresponding virtual IP address in the HOME list as the source IP address for outbound datagrams that do not have an explicit source address. This field can have the following values:

Yes Indicates that SOURCEVIPA is in effect (the SOURCEVIPA parameter was specified in the IPCONFIG profile statement).

No Indicates that SOURCEVIPA is not in effect (the NOSOURCEVIPA parameter was specified in the IPCONFIG profile statement or is in effect by default).

MultiPath
Indicates whether the multipath routing selection algorithm for outbound IP traffic is enabled for this TCP/IP stack. Possible values are:

Pkt Indicates that outbound traffic uses the multipath routes in a round-robin fashion for each outbound packet (the MULTIPATH PERPACKET parameter was specified in the IPCONFIG profile statement).

Conn Indicates that outbound traffic uses the multipath routes in a round-robin fashion for each outbound connection request (the MULTIPATH PERCONNECTION parameter was specified in the IPCONFIG profile statement).

No Indicates that outbound traffic always uses the first active route in a multipath group (the NOMULTIPATH parameter was specified in the IPCONFIG profile statement or is in effect by default).

PathMtuDsc
Indicates whether TCP/IP is to dynamically discover the PMTU, which is the smallest MTU of all the hops in the path. This field can have the following values:

Yes Indicates that PATHMTUDISCOVERY is in effect (the PATHMTUDISCOVERY parameter was specified in the IPCONFIG profile statement),

No Indicates that PATHMTUDISCOVERY is not in effect (the NOPATHMTUDISCOVERY parameter was specified in the IPCONFIG profile statement or is in effect by default).

DevRtryDur
The retry period duration (in seconds) for a failed device or interface

that was defined using the DEVRETRYDURATION parameter in the IPCONFIG statement. TCP/IP performs reactivation attempts at 30 second intervals during this retry period. The default value is 90 seconds. The value 0 indicates an infinite recovery period; reactivation attempts are performed until the device or interface is either successfully reactivated or manually stopped. The maximum value is 4294967295. If the DEVRETRYDURATION parameter was not specified in the IPCONFIG statement, then the default value 90 is displayed.

DynamicXCF
Indicates whether IPv4 XCF dynamic support is enabled for this TCP/IP stack. This field can have the following values:

Yes Indicates that XCF dynamic support is in effect (the DYNAMICXCF parameter was specified in the IPCONFIG profile statement).

No Indicates that XCF dynamic support is not in effect (the NODYNAMICXCF parameter was specified in the IPCONFIG profile statement or is in effect by default).

When XCF dynamic support is in effect, the following information is displayed:

IpAddr
The IPv4 address that was specified for DYNAMICXCF in the IPCONFIG profile statement.

Subnet
The subnet mask that was specified for DYNAMICXCF in the IPCONFIG profile statement.

Guidelines:

1. If the IpAddr/PrefixLen format was used for DYNAMICXCF in the IPCONFIG profile statement, then it is displayed in the same format in the Netstat report. The PrefixLen is the integer value in the range 1 - 32 that represents the number of left-most significant bits for the address mask.
2. If the IPv6_address/prefix_route_len format was used for DYNAMICXCF in the IPCONFIG6 profile statement, then it is displayed in the same format in the Netstat report. The length of routing prefix is an integer value in the range 1 - 128.

Metric The interface routing metric represents the configured cost_metric value to be used by dynamic routing daemons for routing preferences. It is configured using the cost_metric value in the IPCONFIG DYNAMICXCF statement.

SecClass
Indicates the IP Security security class value that is associated with the dynamic XCF link. Valid values are in the range 1 - 255.

SMCD
Indicates whether the HiperSockets interface that dynamic XCF generates supports Shared Memory Communications - Direct Memory Access (SMC-D). This field can have the following values:

Yes Indicates that the HiperSockets interface that dynamic XCF generates can be used for new TCP connections

with SMC-D. The SMCD parameter was specified on the IPCONFIG profile statement or the value was set by default.

No Indicates that the HiperSockets interface that dynamic XCF generates cannot be used for new TCP connections with SMC-D. The NOSMCD parameter was specified on the IPCONFIG profile statement.

SrcVipaInt
The source VIPA interface name that was defined using the DYNAMICXCF SOURCEVIPAINTERFACE parameter in the IPCONFIG statement. It must be a VIRTUAL interface. This field indicates the value No if the SOURCEVIPAINTERFACE subparameter was not specified for the DYNAMICXCF in the IPCONFIG statement.

QDIOAccel
Indicates whether QDIO Accelerator is enabled for this TCP/IP stack. This field can have the following values:

Yes Indicates that the QDIO Accelerator is enabled (the QDIOACCELERATOR parameter was specified in the IPCONFIG profile statement).

SD only
Indicates that the QDIO Accelerator is enabled (the QDIOACCELERATOR parameter was specified in the IPCONFIG profile statement), but only for Sysplex Distributor traffic and not for routed traffic. This might be the case if IP forwarding is disabled on this stack, or if IP filters or defensive filters require this stack to perform special processing for routed traffic. For more information, see QDIO Accelerator and IP security in z/OS Communications Server: IP Configuration Guide.

No Indicates that the QDIO Accelerator is not enabled (the NOQDIOACCELERATOR parameter was specified in the IPCONFIG profile statement or is in effect by default).

QDIOAccelPriority
Indicates which QDIO outbound priority level should be used if the QDIO Accelerator is routing packets to a QDIO device. If the NOQDIOACCELERATOR parameter was specified in the IPCONFIG profile statement or is in effect by default, then the QDIOAccelPriority field is not displayed.

IQDIORoute
Indicates whether HiperSockets Accelerator is enabled for this TCP/IP stack. This field can have the following values:

Yes Indicates that HiperSockets Accelerator is enabled (the IQDIOROUTING parameter was specified in the IPCONFIG profile statement).

No Indicates that HiperSockets Accelerator is not enabled (the NOIQDIOROUTING parameter was specified in the IPCONFIG profile statement or is in effect by default).

n/a Indicates that HiperSockets Accelerator does not apply because QDIO Accelerator is enabled.

QDIOPriority
Indicates which QDIO outbound priority level should be used if the HiperSockets Accelerator is routing packets to a QDIO device. If the NOIQDIOROUTING parameter was specified in the IPCONFIG profile statement or is in effect by default, then the QDIOPriority field is not displayed. This field is displayed only when the IQDIORoute field value is `Yes`.

TcpStackSrcVipa
The IPv4 address that was defined using the TCPSTACKSOURCEVIPA parameter in the IPCONFIG statement. It must be the source IP address for outbound TCP connections if SOURCEVIPA has been enabled. This field has the value `No` if the TCPSTACKSOURCEVIPA parameter was not specified in the IPCONFIG statement

ChecksumOffload
Indicates whether the IPv4 checksum offload function is enabled or disabled. This field can have the following values:

Yes Indicates that the checksum processing for IPv4 packets is offloaded to OSA-Express interfaces that support the checksum offload function. The CHECKSUMOFFLOAD parameter was specified on the IPCONFIG profile statement or the value was set by default.

No Indicates that the checksum processing is performed by the TCP/IP stack. The NOCHECKSUMOFFLOAD parameter was specified on the IPCONFIG profile statement.

SegOffload
Indicates whether the IPv4 TCP segmentation offload function is enabled or disabled. This field can have the following values:

Yes Indicates that IPv4 TCP segmentation is performed by OSA-Express interfaces that support the segmentation offload function. The SEGMENTATIONOFFLOAD parameter was specified on the IPCONFIG profile statement.

No Indicates that the segmentation is performed by the TCP/IP stack. The NOSEGMENTATIONOFFLOAD parameter was specified on the IPCONFIG profile statement or the value was set by default.

- **IPv6 Configuration Table if the TCP/IP stack is IPv6 enabled**

  Displays the following configured IPv6 information that is defined in the IPCONFIG6 profile statement For more information about each IPv6 IP parameter, see the IPCONFIG6 profile statement information in the z/OS Communications Server: IP Configuration Reference.

  Forwarding
  Indicates whether the transfer of data between networks is enabled for this TCP/IP stack. Possible values are:

  Pkt Indicates that packets that are received but that are not destined for this stack are forwarded and use multipath routes if available on a per-packet basis (the DATAGRAMFWD FWDMULTIPATH PERPACKET was specified in the IPCONFIG6 profile statement).

  Yes Indicates that packets that are received but that are not destined for this stack are forwarded but do not use multipath routes even if they are available. (the DATAGRAMFWD

NOFWDMULTIPATH was specified in the IPCONFIG6 profile statement or is in effect by default).

No Indicates that packets that are received but that are not destined for this stack are not forwarded in route to the destination (the NODATAGRAMFWD parameter was specified in the IPCONFIG6 profile statement).

HopLimit
The hop limit value that was defined using the HOPLIMIT parameter in the IPCONFIG6 statement. It is the number of hops that a packet that originates at this host can travel in route to the destination. Valid values are in the range 1 - 255; the default value is 255. If the HOPLIMIT parameter was not specified in the IPCONFIG6 statement, then the default value 255 is displayed.

IgRedirect
Indicates whether TCP/IP is to ignore ICMP Redirect packets. This field can have the following values:

Yes Indicates that IGNOREREDIRECT is in effect. The IGNOREREDIRECT parameter was defined on the IPCONFIG6 profile statement, OMPROUTE has been started and IPv6 interfaces are configured to OMPROUTE, or intrusion detection services (IDS) policy is in effect to detect and discard ICMP Redirects.

No Indicates that ICMP Redirects are not ignored.

SourceVipa
Indicates whether to use a virtual IP address that is assigned to the SOURCEVIPAINT interface as the source address for outbound datagrams that do not have an explicit source address. You must specify the SOURCEVIPAINT parameter on the INTERFACE profile statement for each interface where you want the SOURCEVIPA address to take effect. This field can have the following values:

Yes Indicates that SOURCEVIPA is in effect (the SOURCEVIPA parameter was specified in the IPCONFIG6 profile statement).

No Indicates that SOURCEVIPA is not in effect (the NOSOURCEVIPA parameter was specified in the IPCONFIG6 profile statement or is in effect by default).

MultiPath
Indicates whether the multipath routing selection algorithm for outbound IP traffic is enabled for this TCP/IP stack. Possible values are:

Pkt Indicates that outbound traffic uses the multipath routes in a round-robin fashion for each outbound packet (the MULTIPATH PERPACKET parameter was specified in the IPCONFIG6 profile statement).

Conn Indicates that outbound traffic uses the multipath routes in a round-robin fashion for each outbound connection request (the MULTIPATH PERCONNECTION parameter was specified in the IPCONFIG6 profile statement).

No Indicates that outbound traffic always uses the first active route in a multipath group (the NOMULTIPATH parameter was specified in the IPCONFIG6 profile statement is in effect by default).

IcmperrLim
The ICMP error limit value that was defined using the ICMPERRORLIMIT parameter in the IPCONFIG6 statement. It controls the rate at which ICMP error messages can be sent to a particular IPv6 destination address. The number displayed is the number of messages per second. Valid values are in the range 1 - 20; the default value is 3. If the ICMPERRORLIMIT parameter was not specified in the IPCONFIG6 statement, then the default value 3 is displayed.

IgRtrHopLimit
Indicates whether the TCP/IP stack ignores a hop limit value that is received from a router in a router advertisement. This field can have the following values:

Yes Indicates that IGNOREROUTERHOPLIMIT is in effect (the IGNOREROUTERHOPLIMIT parameter was defined on the IPCONFIG6 profile statement).

No Indicates that IGNOREROUTERHOPLIMIT is not in effect (the NOIGNOREROUTERHOPLIMIT parameter was defined on the IPCONFIG6 profile statement or is in effect by default).

IpSecurity
Indicates whether the IP filtering and IPSec tunnel support is enabled.

Yes Indicates that IP security is in effect (the IPSECURITY parameter was defined on the IPCONFIG6 profile statement). When IP security is in effect, the following information is displayed:

OSMSecClass
Indicates the IP Security security class value that is associated with the OSM interfaces. Valid values are in the range 1 - 255.

No Indicates that IP security is not in effect.

DynamicXCF
Indicates whether IPv6 XCF dynamic support is enabled for this TCP/IP stack. This field can have the following values:

Yes Indicates that XCF dynamic support is in effect (the DYNAMICXCF parameter was specified in the IPCONFIG6 profile statement).

No Indicates that XCF dynamic support is not in effect (the NODYNAMICXCF parameter was specified in the IPCONFIG6 profile statement or is in effect by default).

When XCF dynamic support is in effect, the following information is displayed:

IpAddr
The IPv6 address that was specified for DYNAMICXCF in the IPCONFIG6 profile statement.

Tip: If the IpAddr/PrefixRouteLen format was used for DYNAMICXCF in the IPCONFIG6 profile statement, then it is displayed in the same format in the Netstat report. The PrefixRouteLen is the integer value in the range 1 - 128.

IntfId The 64-bit interface identifier in colon-hexadecimal format that was specified using INTFID subparameter for DYNAMICXCF in

the IPCONFIG6 profile statement. If the INTFID subparameter was not specified, then this field is `not` displayed.

SrcVipaInt
The source VIPA interface name that was defined using the DYNAMICXCF SOURCEVIPAINTERFACE parameter in the IPCONFIG6 statement. It must be a VIRTUAL6 interface. This field indicates the value `No` if the SOURCEVIPAINTERFACE subparameter was not specified for the DYNAMICXCF in the IPCONFIG6 statement.

SecClass
Indicates the IP Security security class value that is associated with the IPv6 dynamic XCF interfaces. Valid values are in the range 1 - 255.

SMCD
Indicates whether the HiperSockets interface that dynamic XCF generates supports SMC-D. This field can have the following values:

Yes Indicates that the HiperSockets interface that dynamic XCF generates can be used for new TCP connections with SMC-D. The SMCD parameter was specified on the IPCONFIG6 profile statement or the value was set by default.

No Indicates that the HiperSockets interface that dynamic XCF generates cannot be used for new TCP connections with SMC-D. The NOSMCD parameter was specified on the IPCONFIG6 profile statement.

TcpStackSrcVipa
The IPv6 interface name that was defined using the TCPSTACKSOURCEVIPA parameter in the IPCONFIG6 statement. It must be the source interface for outbound TCP connections if SOURCEVIPA has been enabled. This field indicates the value `No` if the TCPSTACKSOURCEVIPA parameter was not specified in the IPCONFIG6 statement

TempAddresses
Indicates whether the TCP/IP stack generates IPv6 temporary addresses for IPv6 interfaces for which stateless address autoconfiguration is enabled. This field can have the following values:

Yes Indicates that this behavior is enabled (the TEMPADDRS parameter was defined on the IPCONFIG6 profile statement).

No Indicates that this behavior is not enabled (the NOTEMPADDRS parameter was defined on the IPCONFIG6 profile statement or is in effect by default).

When TEMPADDRS support is in effect, the following information is displayed:

PreferredLifetime
The preferred lifetime for IPv6 temporary addresses, which was defined using the PREFLIFETIME parameter in the IPCONFIG6 statement.

At the expiration of the preferred lifetime, a new temporary address is generated and the existing address is deprecated. The number that is displayed is the preferred lifetime, in hours. Valid values are in the range of 1 - 720 hours (30 days). The default value is 24 hours.

ValidLifetime
The valid lifetime for IPv6 temporary addresses that was defined using the VALIDLIFETIME parameter in the IPCONFIG6 statement.

When the valid lifetime expires, the temporary address is deleted. The number displayed is the valid lifetime in hours. Valid values are in the range 2 - 2160 hours (90 days). The default value is 7 times the preferred lifetime value, with a maximum of 90 days.

ChecksumOffload
Indicates whether the IPv6 checksum offload function is enabled or disabled. This field can have the following values:

Yes Indicates that the checksum processing for IPv6 packets is offloaded to OSA-Express interfaces that support the checksum offload function. The CHECKSUMOFFLOAD parameter was specified on the IPCONFIG6 profile statement or the value was set by default.

No Indicates that the checksum processing is performed by the TCP/IP stack. The NOCHECKSUMOFFLOAD parameter was specified on the IPCONFIG6 profile statement.

SegOffload
Indicates whether the IPv6 TCP segmentation offload function is enabled or disabled. This field can have the following values:

Yes Indicates that the IPv6 TCP segmentation is offloaded to OSA-Express interfaces that support the segmentation offload function. The SEGMENTATIONOFFLOAD parameter was specified on the IPCONFIG6 profile statement.

No Indicates that the segmentation is performed by the TCP/IP stack. The NOSEGMENTATIONOFFLOAD parameter was specified on the IPCONFIG6 profile statement or the value was set by default.

- **SMF parameters**

  Display the following configured SMF information defined in the SMFCONFIG profile statement. For more information about each SMF parameter, see SMFCONFIG profile statement information in the z/OS Communications Server: IP Configuration Reference.

  Type 118

  TcpInit
  Indicates whether SMF subtype 1 records are created when TCP connections are established. A value of the subtype indicates that TYPE118 TCPINIT is in effect (the TCPINIT or TYPE118 TCPINIT was specified on the SMFCONFIG profile statement or a nonzero value of inittype was specified on the SMFPARMS profile statement).

The value 0 indicates that TYPE118 TCPINIT is not in effect (the NOTCPINIT or TYPE118 NOTCPINIT was specified in the SMFCONFIG profile statement (or is in effect by default), or zero value of inittype was specified on the SMFPARMS profile statement).

TcpTerm
Indicates whether SMF subtype 2 records are created when TCP connections are established. A value of the subtype indicates that TYPE118 TCPTERM is in effect (the TCPTERM or TYPE118 TCPTERM was specified on the profile SMFCONFIG statement or a non zero value of termtype was specified on the SMFPARMS profile statement).

The value 0 indicates that TYPE118 TCPTERM is not in effect (the NOTCPTERM or TYPE118 NOTCPTERM was specified in the SMFCONFIG profile statement (or is in effect by default), or zero value of termtype was specified on the SMFPARMS profile statement).

FTPClient
Indicates whether SMF subtype 3 records are created when TCP connections are established. A value of the subtype indicates that TYPE118 FTPCLIENT is in effect (the FTPCLIENT or TYPE118 FTPCLIENT was specified on the SMFCONFIG profile statement or a non zero value of clienttype was specified on the SMFPARMS profile statement).

The value 0 indicates that TYPE118 FTPCLIENT is not in effect (the NOFTPCLIENT or TYPE118 NOFTPCLIENT was specified in the SMFCONFIG profile statement (or is in effect by default), or zero value of clienttype was specified on the SMFPARMS profile statement).

TN3270Client
Indicates whether SMF subtype 4 records are created when TCP connections are established. A value of the subtype indicates TYPE118 TN3270CLIENT is in effect (the TN3270CLIENT or TYPE118 TN3270CLIENT was specified on the SMFCONFIG profile statement or a non zero value of clienttype was specified on the SMFPARMS profile statement).

The value 0 indicates that TYPE118 TN3270CLIENT is not in effect (the NOTN3270CLIENT or TYPE118 NOTN3270CLIENT was specified in the SMFCONFIG profile statement (or is in effect by default), or zero value of clienttype was specified on the SMFPARMS profile statement).

TcpIpStates
Indicates whether SMF subtype 5 records are created when TCP connections are established. A value of the subtype indicates that TYPE118 TCPIPSTATISTICS is in effect (the TCPIPSTATISTICS or TYPE118 TCPIPSTATISTICS was specified on the SMFCONFIG statement).

The value 0 indicates that TYPE118 TCPIPSTATISTICS is not in effect (the NOTCPIPSTATISTICS or TYPE118 NOTCPIPSTATISTICS was specified in the SMFCONFIG profile statement or is in effect by default).

Type 119

TcpInit
Indicates whether SMF records of subtype 1 are created when TCP connections are established. This field can have the following values:

Yes Indicates that TYPE119 TCPINIT is in effect (the TYPE119 TCPINIT was specified on the SMFCONFIG statement).

No Indicates that TYPE119 TCPINIT is not in effect (the TYPE119 NOTCPINIT was specified in the SMFCONFIG profile statement or is in effect by default).

TcpTerm
Indicates whether SMF subtype 2 records are created when TCP connections are established. This field can have the following values:

Yes Indicates that TYPE119 TCPTERM is in effect (the TYPE119 TCPTERM was specified on the SMFCONFIG statement).

No Indicates that TYPE119 TCPTERM is not in effect (the TYPE119 NOTCPTERM was specified in the SMFCONFIG profile statement or is in effect by default).

FTPClient
Indicates whether SMF subtype 3 records are created when TCP connections are established. This field can have the following values:

Yes Indicates that TYPE119 FTPCLIENT is in effect (the TYPE119 FTPCLIENT was specified on the SMFCONFIG statement).

No Indicates that TYPE119 FTPCLIENT is not in effect (the TYPE119 NOFTPCLIENT was specified in the SMFCONFIG profile statement or is in effect by default).

TcpIpStats
Indicates whether SMF subtype 5 records are created when TCP connections are established. This field can have the following values:

Yes Indicates that TYPE119 TCPIPSTATISTICS is in effect (the TYPE119 TCPIPSTATISTICS was specified on the SMFCONFIG statement).

No Indicates that TYPE119 TCPIPSTATISTICS is not in effect (the TYPE119 NOTCPIPSTATISTICS was specified in the SMFCONFIG profile statement or is in effect by default).

IfStats Indicates whether SMF subtype 6 and subtype 44 records are created. This field can have the following values:

Yes Indicates that TYPE119 IFSTATISTICS is in effect (the TYPE119 IFSTATISTICS was specified on the SMFCONFIG statement).

No Indicates that TYPE119 IFSTATISTICS is not in effect (the

TYPE119 NOIFSTATISTICS was specified in the SMFCONFIG profile statement or is in effect by default).

PortStats
Indicates whether SMF subtype 7 records are created when TCP connections are established. This field can have the following values:

Yes Indicates that TYPE119 PORTSTATISTICS is in effect (the TYPE119 PORTSTATISTICS was specified on the SMFCONFIG statement).

No Indicates that TYPE119 PORTSTATISTICS is not in effect (the TYPE119 NOPORTSTATISTICS was specified in the SMFCONFIG profile statement or is in effect by default).

Stack Indicates whether SMF subtype 8 records are created when TCP connections are established. This field can have the following values:

Yes Indicates that TYPE119 TCPSTACK is in effect (the TYPE119 TCPSTACK was specified on the SMFCONFIG statement).

No Indicates that TYPE119 TCPSTACK is not in effect (the TYPE119 NOTCPSTACK was specified in the SMFCONFIG profile statement or is in effect by default).

UdpTerm
Indicates whether SMF subtype 10 records are created when TCP connections are established. This field can have the following values:

Yes Indicates that TYPE119 UDPTERM is in effect (the TYPE119 UDPTERM was specified on the SMFCONFIG statement).

No Indicates that TYPE119 UDPTERM is not in effect (the TYPE119 NOUDPTERM was specified in the SMFCONFIG profile statement or is in effect by default).

TN3270Client
Indicates whether SMF subtype 22 and 23 records are created when TCP connections are established. This field can have the following values:

Yes Indicates that TYPE119 TN3270CLIENT is in effect (the TYPE119 TN3270CLIENT was specified on the SMFCONFIG statement).

No Indicates that TYPE119 TN3270CLIENT is not in effect (the TYPE119 NOTN3270CLIENT was specified in the SMFCONFIG profile statement or is in effect by default).

IPSecurity
Indicates whether SMF records of subtypes 77, 78, 79, and 80 are created when dynamic tunnels are removed and when manual tunnels are activated and deactivated. This field can have the following values:

Yes Indicates that TYPE119 IPSECURITY is in effect (the TYPE119 IPSECURITY was specified on the SMFCONFIG statement).

No Indicates that TYPE119 IPSECURITY is not in effect (the TYPE119 NOIPSECURITY was specified or is in effect by default in the SMFCONFIG profile statement).

Profile

Indicates whether SMF subtype 4 event records are created when the TCP/IP stack is initialized or when a profile change occurs. This record provides TCP/IP stack profile information. This field can have the following values:

Yes Indicates that this behavior is enabled (the TYPE119 PROFILE parameter was specified on the SMFCONFIG statement).

No Indicates that this behavior is not enabled (the TYPE119 NOPROFILE parameter was specified on the SMFCONFIG statement or is in effect by default).

DVIPA

Indicates whether SMF subtypes 32, 33, 34, 35, 36, and 37 event records are created for sysplex events. These records provide information about changes to dynamic virtual IP addresses (DVIPAs), DVIPA targets, and DVIPA target servers. This field can have the following values:

Yes Indicates that this behavior is enabled (the TYPE119 DVIPA parameter was specified on the SMFCONFIG statement).

No Indicates that this behavior is not enabled (the TYPE119 NODVIPA parameter was specified on the SMFCONFIG statement or is in effect by default).

SmcrGrpStats

Indicates whether SMF subtype 41 records are created. These records are SMC-R link group statistics records. The records collect information about Shared Memory Communications over Remote Direct Memory Access (SMC-R) link groups and the SMC-R links within each group. This field can have the following values:

Yes Indicates that this behavior is enabled. The TYPE119 SMCRGROUPSTATISTICS parameter was specified on the SMFCONFIG statement.

No Indicates that this behavior is not enabled. The TYPE119 NOSMCRGROUPSTATISTICS parameter was specified on the SMFCONFIG statement or is in effect by default.

SmcrLnkEvent

Indicates whether SMF subtype 42 and 43 records are created. The SMF records of subtype 42 are created when SMC-R links are started, and the SMF records of subtype 43 are created when SMC-R links are ended. This field can have the following values:

Yes Indicates that this behavior is enabled. The TYPE119 SMCRLINKEVENT parameter was specified on the SMFCONFIG statement.

No Indicates that this behavior is not enabled. The TYPE119 NOSMCRLINKEVENT parameter was specified on the SMFCONFIG statement or is in effect by default.

Note: The TCPIP statistics field under SMF Parameters displays the subtype value used when creating the SMF type 118 record (if the value is nonzero). The TCPIP statistics field under Global Configuration Information indicates whether the TCP/IP stack will write statistics messages to the TCP/IP job log when TCP/IP is terminated. For the Type 119 fields, the subtype cannot be changed and the setting indicates if the record is requested (Yes) or not (No).

- **Global Configuration Information**

  Display the following global configured information defined in the GLOBALCONFIG profile statement. For more information about each global parameter, see GLOBALCONFIG profile statement information in the z/OS Communications Server: IP Configuration Reference.

  TcpIpStats
  Indicates whether the several TCP/IP counter values are to be written to the output data set designated by the CFGPRINT JCL statement. The value Yes indicates that TCPIPSTATISTICS is in effect (the TCPIPSTATISTICS parameter was specified in the GLOBALCONFIG profile statement). The value No indicates that TCPIPSTATISTICS is not in effect (the NOTCPIPSTATISTICS parameter was specified in the GLOBALCONFIG profile statement or is in effect by default).

  Tip: The TCPIPSTATS field that is shown under the SMF PARAMETERS section of the Netstat CONFIG/**-f** output reflects the TcpIpStatistics value or NoTcpIpStatistics value that is specified on the SMFCONFIG statement in the TCP/IP Profile or Obeyfile. The TCPIPSTATS field that is shown under the GLOBAL CONFIGURATION section of the Netstat CONFIG/**-f** output reflects the value from the GLOBALCONFIG statement in the TCP/IP Profile or Obeyfile.

  ECSALimit
  The maximum amount of extended common service area (ECSA) that was defined using the ECSALIMIT parameter in the GLOBALCONFIG statement. This limit can be expressed as a number followed by the letter K (which represents 1024 bytes), or a number followed by the letter M (which represents 1048576 bytes). If the K suffix is used, then the value displayed must be in the range 10240K - 2096128K inclusive, or 0K. If the M suffix is used, the value displayed must be in the range 10M - 2047M inclusive, or 0K. If the ECSALIMIT parameter was not specified in the GLOBALCONFIG statement, then the default value 0K is displayed (which means no limit).

  PoolLimit
  The maximum amount of authorized private storage that was defined using the POOLLIMIT parameter in the GLOBALCONFIG statement. This limit can be expressed as a number followed by the letter K (which represents 1024 bytes), or a number followed by the letter M (which represents 1048576 bytes). If the K suffix is used, then the value displayed must be in the range 10240K to 2096128K inclusive, or 0K. If the M suffix is used, value is displayed must be in the range 10M - 2047M inclusive, or 0K. If the POOLLIMIT parameter was not specified in the GLOBALCONFIG statement, then the default value 0K is displayed (which means no limit).

  MlsChkTerm
  Indicates whether the stack should be terminated when inconsistent configuration information is discovered in a multilevel-secure environment. The value `Yes` indicates that MLSCHKTERMINATE is in effect (the MLSCHKTERMINATE parameter was specified in the

GLOBALCONFIG profile statement). The value No indicates that MLSCHKTERMINATE is not in effect (the NOMLSCHKTERMINATE parameter was specified in the GLOBALCONFIG profile statement or is in effect by default).

XCFGRPID
Displays the TCP 2-digit XCF group name suffix. The two digits displayed are used to generate the XCF group that the TCP/IP stack has joined. The group name is EZBT*vvtt*, where *vv* is the VTAM XCF group ID suffix (specified as a VTAM start option) and *tt* is the displayed XCFGRPID value. If no VTAM XCF group ID suffix was specified, the group name is EZBTCP*tt*. You can use the D TCPIP,,SYSPLEX,GROUP command to display the group name that the TCP/IP stack has joined.

These digits are also used as a suffix for the EZBDVIPA and EZBEPORT structure names in the form EZBDVIPA*vvtt* and EZBEPORT*vvtt*. If no VTAM XCF group ID suffix was specified, the structure names are EZBDVIPA01*tt* and EZBEPORT01*tt*. If no XCFGRPID value was specified on the GLOBALCONFIG statement in the TCP/IP profile, then no value is displayed for XCFGRPID field in the Netstat output.

IQDVLANID
Displays the TCP/IP VLAN ID that is to be used when a HiperSockets link or interface is generated for dynamic XCF connectivity between stacks on the same CPC. The VLAN ID provides connectivity separation between TCP/IP stacks using HiperSockets for dynamic XCF when subplexing is being used (when XCFGRPID was specified on the GLOBALCONFIG statement). TCP/IP stacks with the same XCFGRPID value (stacks in the same subplex) should specify the same IQDVLANID value if the stacks are in the same CPC and use the same CHPID value. TCP/IP stacks with different XCFGRPID values should specify different IQDVLANID values if the stacks are in the same CPC and use the same CHPID value. If no IQDVLANID value was specified on the GLOBALCONFIG statement in the TCP/IP profile, then the value 0 (no value) is displayed for the IQDVLANID field in the Netstat output.

SysplexWLMPoll
The rate, in seconds, at which the sysplex distributor and its target servers poll WLM for new weight recommendations. A shorter rate indicates a quicker response; however, shorter rates might result in unneeded queries.

MaxRecs
The maximum number of records that are displayed by the DISPLAY TCPIP,,NETSTAT operator command, if the MAX parameter is not specified on that command. The maximum number of records is specified on the MAXRECS parameter of the GLOBALCONFIG profile statement. An asterisk (*) indicates that all records are displayed.

ExplicitBindPortRange
The range of ephemeral ports that is assigned uniquely across the sysplex when an explicit bind() is issued using INADDR_ANY or the unspecified IPv6 address (in6addr_any) and when the specified port is 0.

Tip: This range is the range that was configured on this stack. It might not be the actual range that is in use throughout the sysplex at this time, because another stack that was started later with a different explicit bind port range configured (or with a VARY OBEYFILE command specifying a file with a different EXPLICITBINDPORTRANGE value) can override

the range that is configured by this stack. Use the Display TCPIP,,SYSPLEX,PORTS command to display the currently active port range.

AutoIQDX
Indicates whether dynamic Internal Queued Direct I/O extensions function (IQDX) interfaces are used for connectivity to the intraensemble data network (IEDN). This field can have the following values:

No Indicates that access to the IEDN using HiperSockets (IQD CHPIDs) with the IQDX is disabled. The NOAUTOIQDX parameter was specified on the GLOBALCONFIG statement.

AllTraffic
Indicates that IQDX interfaces are used for all eligible outbound traffic to the IEDN. The AUTOIQDX ALLTRAFFIC parameter was specified on the GLOBALCONFIG statement. This value is the default value for the AutoIQDX field.

NoLargeData
Indicates that IQDX interfaces are used for all eligible outbound traffic to the IEDN, except for large outbound TCP protocol traffic. The AUTOIQDX NOLARGEDATA parameter was specified on the GLOBALCONFIG statement. Large outbound TCP traffic is sent to the IEDN by using OSX OSA-Express interfaces.

IQDMultiWrite
Indicates whether all HiperSockets interfaces are configured to move multiple output data buffers using a single write operation. You must stop and restart the interface for a change in this value to take effect for an active HiperSockets interface. This field can have the following values:

Yes Indicates that the HiperSockets interfaces are configured to use HiperSockets multiple write support when this function is supported by the IBM z Systems™ environment (the IQDMULTIWRITE parameter was specified on the GLOBALCONFIG profile statement).

No Indicates that the HiperSockets interfaces are not configured to use HiperSockets multiple write support (the NOIQDMULTIWRITE parameter was specified on the GLOBALCONFIG profile statement or the value was set by default).

WLMPriorityQ
Indicates whether OSA-Express QDIO write priority values are being assigned to outbound OSA-Express packets that are associated with Workload Manager (WLM) service classes, and to forwarded packets that are not being accelerated. The displayed priorities are applied only when the IPv4 type of service (ToS) byte or the IPv6 traffic class value in the IP header is 0 and the packet is sent from an OSA-Express device that is in QDIO mode. This field can have the following values:

Yes Indicates that QDIO write priority values are assigned to outbound OSA-Express packets that are associated with Workload Manager (WLM) service classes, and to forwarded packets that are not being accelerated (the WLMPRIORITYQ parameter was specified on the GLOBALCONFIG profile

statement). When the WLMPriorityQ field has the value Yes, the following information is displayed:

IOPRIn control_values
Indicates which QDIO priority value is assigned to each control value. The QDIO priority values are in the range of 1 - 4. These QDIO priority values are displayed as the identifiers IOPRI1, IOPRI2, IOPRI3, and IOPRI4. The values that follow the identifiers are the control values. The control values represent Workload Manager service classes and forwarded packets. Most of the control values correlate directly to Workload Manager service class importance levels. See the WLMPRIORITYQ parameter in the GLOBALCONFIG profile statement information in z/OS Communications Server: IP Configuration Reference for more details about the control values. If no control value was specified for a specific QDIO priority value, then the identifier for that QDIO priority value is not displayed.

No Indicates that QDIO write priority values are not assigned to outbound OSA-Express packets that are associated with Workload Manager (WLM) service classes or to forwarded packets that are not accelerated (the NOWLMPRIORITYQ parameter was specified on the GLOBALCONFIG profile statement or is in effect by default).

Sysplex Monitor
Displays the parameter values for the Sysplex Problem Detection and Recovery function.

TimerSecs
Displays the timer value (in seconds) that is used to determine how soon the sysplex monitor timer reacts to problems with needed sysplex resources. This value can be configured using the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement. Valid values are in the range 10 - 3600 seconds; the default value is 60 seconds.

Recovery
Indicates the action that is to be taken when a sysplex problem is detected.

The value Yes indicates that when a problem is detected, the stack issues messages about the problem, leaves the sysplex group, and deactivates all DVIPA resources that are owned by this stack; the VIPADYNAMIC configuration is restored if the stack rejoins the sysplex group. The default value is No. The value Yes can be configured by specifying the RECOVERY keyword for the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

The value No indicates that when a problem is detected, the stack issues messages regarding the problem but takes no other action. The value No can be configured by specifying the NORECOVERY keyword for the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

DelayJoin
Indicates whether the TCP/IP stack delays joining the sysplex

group during stack initialization or rejoining the sysplex group following a VARY TCPIP,,OBEYFILE command.

The value `No` indicates that TCP/IP immediately joins the sysplex group during stack initialization. The default value is `No` and can be configured by specifying the NODELAYJOIN keyword for the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

The value `Yes` indicates that TCP/IP delays joining the sysplex group during stack initialization until the following conditions true:

- OMPROUTE is started and active
- At least one of monitored interfaces is defined and active (if MONINTERFACE is configured)
- At least one dynamic route over the monitored interfaces is available (if MONINTERFACE DYNROUTE is configured)

Any sysplex-related definitions within the TCP/IP profile (for example, VIPADYNAMIC or IPCONFIG/IPCONFIG6 DYNAMICXCF statements) are not processed until the sysplex group is joined. The value `Yes` can be configured by specifying the DELAYJOIN keyword for the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

Join Indicates whether the TCP/IP stack joins the sysplex group during stack initialization.

The value `Yes` indicates that the TCP/IP stack immediately attempts to join the sysplex group during stack initialization. This is the default setting.

The value `No` indicates that the TCP/IP stack does not join the sysplex group during stack initialization. You can configure the value `No` by specifying the NOJOIN keyword for the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

If NOJOIN is configured, the TCP/IP stack does not process any VIPADYNAMIC block or DYNAMICXCF statements. Any other GLOBALCONFIG SYSPLEXMONITOR parameter settings (configured or default) are ignored, and the settings are saved in case you want the TCP/IP stack to join the sysplex group at a later time.

If you subsequently issue a VARY TCPIP,,SYSPLEX,JOINGROUP command, the NOJOIN setting is overridden and the saved GLOBALCONFIG SYSPLEXMONITOR parameter settings become active. For example, if you configure NOJOIN and DELAYJOIN, DELAYJOIN is initially ignored. After you issue a V TCPIP,,SYSPLEX,JOINGROUP command, NOJOIN is overridden, DELAYJOIN becomes active, and the stack joins the sysplex group if OMPROUTE is initialized.

Any sysplex-related definitions within the TCP/IP profile, such as VIPADYNAMIC or IPCONFIG DYNAMICXCF statements, are not processed until the TCP/IP stack joins the sysplex group.

MonIntf
Indicates whether the TCP/IP stack is monitoring the status of specified network interfaces.

The value `No` indicates that the TCP/IP stack is not monitoring the status of network interfaces. The default value is `No` and it can be configured by specifying the NOMONINTERFACE keyword for the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

The value `Yes` indicates that the TCP/IP stack is monitoring the status of network interfaces that have the MONSYSPLEX attribute specified on the LINK or INTERFACE profile statement. The value `Yes` can be configured by specifying the MONINTERFACE keyword for the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

DynRoute
Indicates whether the TCP/IP stack is monitoring the presence of dynamic routes over the monitored network interfaces.

The value `No` indicates that the TCP/IP stack is not monitoring the presence of dynamic routes over monitored network interfaces. The default value is `No` and it can be configured by specifying the NODYNROUTE keyword for the SYSPLEXMONITOR MONINTERFACE parameter on the GLOBALCONFIG profile statement.

The value `Yes` indicates that the TCP/IP stack is monitoring the presence of dynamic routes over monitored network interfaces that have the MONSYSPLEX attribute specified on the LINK or INTERFACE statement. It can be configured by specifying the DYNROUTE keyword for the SYSPLEXMONITOR MONINTERFACE parameter on the GLOBALCONFIG profile statement.

AutoRejoin
Indicates whether the TCP/IP stack automatically rejoins the sysplex group when all detected problems that caused the stack to leave the group are relieved.

The value `No` indicates that the stack does not rejoin the group or restore its VIPADYNAMIC definitions when all detected problems have been relieved. The default value is `No` and it can be configured by specifying the NOAUTOREJOIN keyword for the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

The value `Yes` indicates that the stack automatically rejoins the sysplex group and restores all of its VIPADYNAMIC configuration definitions. The value `Yes` can be configured by specifying the AUTOREJOIN keyword for the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

Restriction: You can specify the AUTOREJOIN keyword only if the RECOVERY keyword is also specified (or is currently enabled) on the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

zIIP Displays information about displacing CPU cycles for various functions

onto a System z Information Integration Processor (zIIP). The value Yes for a function indicates that cycles can be displaced to a zIIP when at least one zIIP device is online. Issue the MVS D M=CPU command to display zIIP status. See displaying system configuration information details in z/OS MVS System Commands for more information about displaying processor status.

IPSecurity
Indicates whether the stack is configured to displace CPU cycles for IPSec workload onto a zIIP. This field can have the following values:

Yes Indicates that IPSec CPU cycles are displaced to a zIIP as long as at least one zIIP device is online.

No Indicates that IPSec CPU cycles are not being displaced to a zIIP.

IQDIOMultiWrite
Indicates whether the stack is configured to displace CPU cycles for HiperSockets multiple write workload onto a zIIP. This field can have the following values:

Yes Indicates that the stack is configured to permit HiperSockets multiple write CPU cycles to be displaced to a zIIP.

No Indicates that the stack is configured to not permit HiperSockets multiple write CPU cycles to be displaced to a zIIP.

SMCGlobal
Displays the global settings for Shared Memory Communications (SMC). SMC includes Shared Memory Communications over Remote Direct Memory Access (RDMA), or SMC-R, for external data network communications and Shared Memory Communications - Direct Memory Access (SMC-D). This field has the following values:

AutoCache
Indicates whether AUTOCACHE support is enabled for this TCP/IP stack. The following values are valid:

Yes Indicates that AUTOCACHE support is enabled. The AUTOCACHE subparameter was specified with the SMCGLOBAL parameter on the GLOBALCONFIG profile statement or AUTOCACHE support is enabled by default. This support is started only when SMC is enabled. SMC is enabled if the value of either the SMCR or the SMCD field is Yes.

No Indicates that AUTOCACHE support is not enabled. The NOAUTOCACHE subparameter was specified with the SMCGLOBAL parameter on the GLOBALCONFIG profile statement.

AutoSMC
Indicates whether the AUTOSMC monitoring function is enabled for this TCP/IP stack. For more information about the AUTOSMC monitoring function, see AUTOSMC monitoring function in z/OS Communications Server: IP Configuration Guide. The following values are valid:

Yes Indicates that the AUTOSMC monitoring function is enabled. The AUTOSMC subparameter was specified with the SMCGLOBAL parameter on the GLOBALCONFIG profile statement or the AUTOSMC monitoring function was enabled by default. This function is started only when SMC is enabled. SMC is enabled if the value of either the SMCR or the SMCD field is Yes.

No Indicates that the AUTOSMC monitoring function is not enabled. The NOAUTOSMC subparameter was specified with the SMCGLOBAL parameter on the GLOBALCONFIG profile statement.

SMCR

Indicates whether this stack supports Shared Memory Communications over Remote Direct Memory Access (SMC-R) for external data network communications. This field can have the following values:

Yes Indicates that this stack can communicate with other stacks on the external data network by using SMC-R. The SMCR parameter was specified on the GLOBALCONFIG profile statement. When the `SMCR` field has the value `Yes`, the following information is displayed:

FixedMemory
Indicates the maximum amount, in megabytes, of 64-bit private storage that the stack can use for the send and receive buffers that are required for SMC-R communications. The fixed memory value was defined by using the SMCR FIXEDMEMORY parameter on the GLOBALCONFIG. If the SMCR FIXEDMEMORY parameter was not specified on the GLOBALCONFIG statement, the default value of 256 is displayed.

TcpKeepMinInt
Indicates the minimum supported TCP keepalive interval for SMC-R links. Use the SMCR TCPKEEPMININTERVAL parameter on the GLOBALCONFIG statement to define the interval. For applications that are using the TCP_KEEPALIVE setsockopt() option, this interval indicates the minimum interval that TCP keepalive packets are sent on the TCP path of an SMC-R link. The range is 0 - 2147460 seconds. If the interval value is set to 0, TCP keepalive probe packets on the TCP path of an SMC-R link are disabled. If the SMCR TCPKEEPMININTERVAL parameter was not specified on the GLOBALCONFIG statement, then the default interval value of 300 is displayed.

PFID Indicates the Peripheral Component Interconnect Express (PCIe) function ID (PFID) value that was defined using SMCR PFID parameter. The combination of PFID and port number uniquely identifies an 10GbE RoCE Express interface. The stack uses 10GbE RoCE Express features for SMC-R communications with other stacks on the external data network. The PFID is a 2-byte hexadecimal value.

PortNum
Indicates the 10GbE RoCE Express port number that is used for the associated PFID. The PortNum value was specified with the PFID value on the SMCR parameter of the GLOBALCONFIG statement in the TCP/IP profile. The port number can be 1 or 2; the default port is 1.

MTU Indicates the configured maximum transmission unit (MTU) value that is used for the associated PFID. The MTU value can be 1024 or 2048 and the default MTU value is 1024.

No Indicates that this stack cannot communicate with other stacks on the external data network by using SMC-R communications. The NOSMCR parameter was specified on the GLOBALCONFIG profile statement or the value was set by default.

SMCD
Indicates whether this stack supports SMC-D. This field can have the following values:

Yes Indicates that this stack can communicate with other stacks by using SMC-D. The SMCD parameter was specified on the GLOBALCONFIG profile statement. When the `SMCD` field has the value `Yes`, the following information is displayed:

FixedMemory
Indicates the maximum amount, in megabytes, of 64-bit private storage that the stack can use for the receive buffers that are required for SMC-D communications. The fixed memory value was defined by using the SMCD FIXEDMEMORY parameter on the GLOBALCONFIG statement. If the SMCD FIXEDMEMORY parameter was not specified on the GLOBALCONFIG statement, the default value of 256 is displayed.

TcpKeepMinInt
Indicates the minimum supported TCP keepalive interval for SMC-R links. Use the SMCD TCPKEEPMININTERVAL parameter on the GLOBALCONFIG statement to define the interval. For applications that are using the TCP_KEEPALIVE setsockopt() option, this interval indicates the minimum interval that TCP keepalive packets are sent on the TCP path of an SMC-D link. The range is 0 - 2147460 seconds. If the interval value is set to 0, TCP keepalive probe packets on the TCP path of an SMC-D link are disabled. If the SMCD TCPKEEPMININTERVAL parameter was not specified on the GLOBALCONFIG statement, the default interval value of 300 is displayed.

No Indicates that this stack cannot communicate with other stacks by using SMC-D communications. The NOSMCD parameter was specified on the GLOBALCONFIG profile statement or the value was set by default.

- **Network Monitor Configuration information**

  Display the following configured network monitor information defined in the NETMONITOR profile statement. For more information about each network

monitor parameter, see the NETMONITOR profile statement information in the z/OS Communications Server: IP Configuration Reference.

PktTrcSrv
Indicates whether the packet trace service is enabled or disabled. The value `Yes` indicates that PKTTRCSERVICE is in effect (the PKTTRCSERVICE parameter was specified in the NETMONITOR profile statement). The value `No` indicates that PKTTRCSERVICE is not in effect (the NOPKTTRCSERVICE parameter was specified in the NETMONITOR profile statement or is in effect by default).

TcpCnnSrv
Indicates whether the TCP connection information service is enabled or disabled. The value `Yes` indicates that TCPCONNSERVICE is in effect (the TCPCONNSERVICE parameter was specified in the NETMONITOR profile statement). The value `No` indicates that TCPCONNSERVICE is not in effect (the NOTCPCONNSERVICE parameter was specified in the NETMONITOR profile statement or is in effect by default).

MinLifTim
The minimum lifetime for a new TCP connection to be reported by the service when the TCP connection information service is enabled. If the NOTCPCONNSERVICE parameter was specified in the NETMONITOR profile statement or is in effect by default, then the MinLifTim field is not displayed.

NtaSrv
Indicates whether the OSAENTA trace service is enabled or disabled. The value `Yes` indicates that NTATRCSERVICE is in effect (the NTATRCSERVICE parameter was specified in the NETMONITOR profile statement). The value `No` indicates that NTATRCSERVICE is not in effect (the NONTATRCSERVICE parameter was specified in the NETMONITOR profile statement or is in effect by default).

SmfSrv
Indicates whether the real-time SMF information service is enabled or disabled. The value `Yes` indicates that SMFSERVICE is enabled (the SMFSERVICE parameter was specified in the NETMONITOR profile statement). The value `No` indicates that SMFSERVICE is disabled (the NOSMFSERVICE parameter was specified in the NETMONITOR profile statement or is disabled by default).

IPSecurity
Indicates whether the real-time SMF service is providing IPSec SMF records. The value `Yes` indicates that IPSec SMF records are being provided (either the SMFSERVICE parameter was specified with the IPSECURITY subparameter on the NETMONITOR profile statement or the SMFSERVICE parameter was specified without any subparameters). The value `No` indicates that IPSec SMF records are not being provided (the SMFSERVICE parameter was specified with the NOIPSECURITY subparameter on the NETMONITOR profile statement). This field is displayed only if the SmfSrv value is `Yes`.

Profile
Indicates whether the real-time SMF service is providing TCP/IP profile SMF records. The value `Yes` indicates that TCP/IP profile SMF records are being provided (either the SMFSERVICE parameter was specified with the PROFILE subparameter on the

NETMONITOR profile statement, or the SMFSERVICE parameter was specified without any subparameters). The value `No` indicates that TCP/IP profile SMF records are not being provided (the SMFSERVICE parameter was specified with the NOPROFILE subparameter on the NETMONITOR profile statement). This field is displayed only if the SmfSrv value is `Yes`.

CSSMTP
Indicates whether the real-time SMF service is providing CSSMTP SMF 119 records for subtype 48, 49, 51 and 52. The value YES indicates that CSSMTP SMF records are being provided (either the SMFSERVICE parameter was specified with the CSSMTP subparameter on the NETMOINTOR profile statement or the SMFSERVICE parameter was specified without any sub parameters). The value NO indicates that CSSMTP SMF records are not being provided (the SMFSERVICE parameter was specified with the NOCSSMTP subparameter on the NETMONITOR profile statement). This field is displayed only if the SMFSrv value is YES.

CSMAIL
Indicates whether the real-time SMF service is providing CSSMTP SMF 119 records for subtype 50. The value YES indicates that CSSMTP SMF mail records are being provided (either the SMFSERVICE parameter was specified with the CSSMTP subparameter on the NETMOINTOR profile statement or the SMFSERVICE parameter was specified without any subparameters). The value NO indicates that CSSMTP SMF mail records are not being provided (the SMFSERVICE parameter was specified with the NOCSSMTP subparameter on the NETMONITOR profile statement). This field is displayed only if the SMFSrv value is YES.

DVIPA
Indicates whether the real-time SMF service is providing sysplex event SMF records. The value `Yes` indicates that sysplex event SMF records are being provided (either the SMFSERVICE parameter was specified with the DVIPA subparameter on the NETMONITOR profile statement, or the SMFSERVICE parameter was specified without any subparameters). The value `No` indicates that sysplex event SMF records are not being provided (the SMFSERVICE parameter was specified with the NODVIPA subparameter on the NETMONITOR profile statement). This field is displayed only if the SmfSrv value is `Yes`.

- **Autolog Configuration Information**

  WaitTime
  The time, displayed in seconds, that is specified on the AUTOLOG statement that represents the length of time TCP/IP waits for a procedure to stop if the procedure is still active at startup and TCP/IP is attempting to start the procedure again. The procedure could still be active if it did not stop when TCP/IP was last shut down.

  ProcName
  The procedure that the TCP/IP address space starts.

JobName
The job name used for the PORT reservation statement. The job name might be identical to the procedure name; however, for z/OS UNIX jobs that spawn listener threads, the names are not the same.

ParmString
A string to be added following the START ProcName value. The ParmString value can be up to 115 characters in length and can span multiple lines. If the PARMSTRING parameter on the AUTOLOG profile statement was not specified or if the *parm_string* value was specified with a blank string, then this field displays blanks.

DelayStart
Indicates whether TCP/IP delays starting this procedure until the TCP/IP stack has completed one or more processing steps. This field can have the following values:

Yes Indicates that the TCP/IP stack does not start this procedure until it has completed all of the processing steps identified by the following subparameters:

DVIPA
TCP/IP delays starting this procedure until after the TCP/IP stack has joined the sysplex group and processed its dynamic VIPA configuration (DELAYSTART was specified on the entry for this procedure in the AUTOLOG profile statement with no additional subparameters, or DELAYSTART was specified with the DVIPA subparameter).

TTLS TCP/IP delays starting this procedure until after the Policy Agent has successfully installed the AT-TLS policy in the TCP/IP stack and AT-TLS services are available (DELAYSTART was specified with the TTLS subparameter on the entry for this procedure in the AUTOLOG profile statement).

No Indicates that this procedure is started when TCP/IP is started (DELAYSTART was not specified on the entry for this procedure in the AUTOLOG profile statement).

- **Data Trace Settings if socket data trace is on**

JobName
The application address space name specified on the DATTRACE command or asterisk (*), if not specified.

TrRecCnt
The number of packets traced for this DATTRACE command.

Length
The value of the ABBREV keyword of the DATTRACE command or FULL to capture the entire packet.

IpAddr
The IP address from the IP keyword of the DATTRACE command or asterisk (*), if not specified.

SubNet
The subnet mask from the SUBNET keyword of the DATTRACE command or asterisk (*), if not specified.

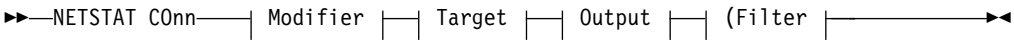
PrefixLen
The prefix length specified on the DATTRACE command.

PortNum
The port number from the PORTNUM keyword of the DATTRACE command or an asterisk (*), if a value was not specified.

Netstat COnn/-c report

Displays the information about each active TCP connection and UDP socket. COnn/**-c** is the default parameter.

TSO syntax



Modifier

APPLDATA
Provides application data in the output report.

SERVER
Provide detailed information only for TCP connections in the listen state.

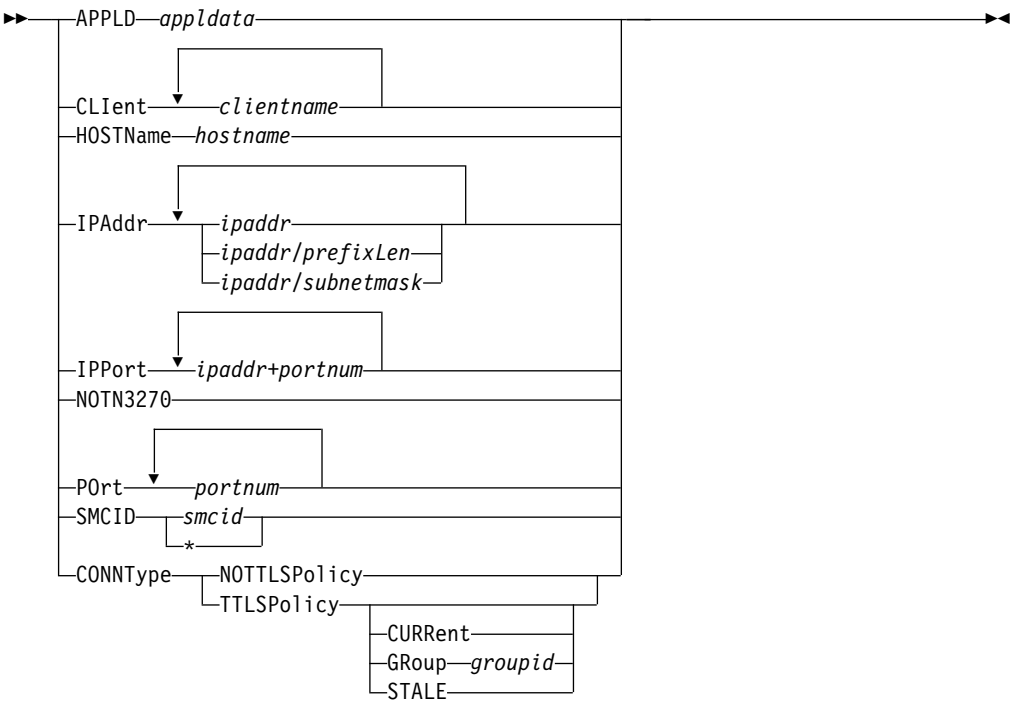
Target

Provide the report for a specific TCP/IP address space by using TCp *tcpname*. See The Netstat command target for more information about the TCp parameter.

Output

The default output option displays the output on the user's terminal. For other options, see “The TSO NETSTAT command syntax” on page 241 or Netstat command output.

Filter



z/OS UNIX syntax

Modifier

APPLDATA
Provides application data in the output report.

SERVER
Provide detailed information only for TCP connections in the listen state.

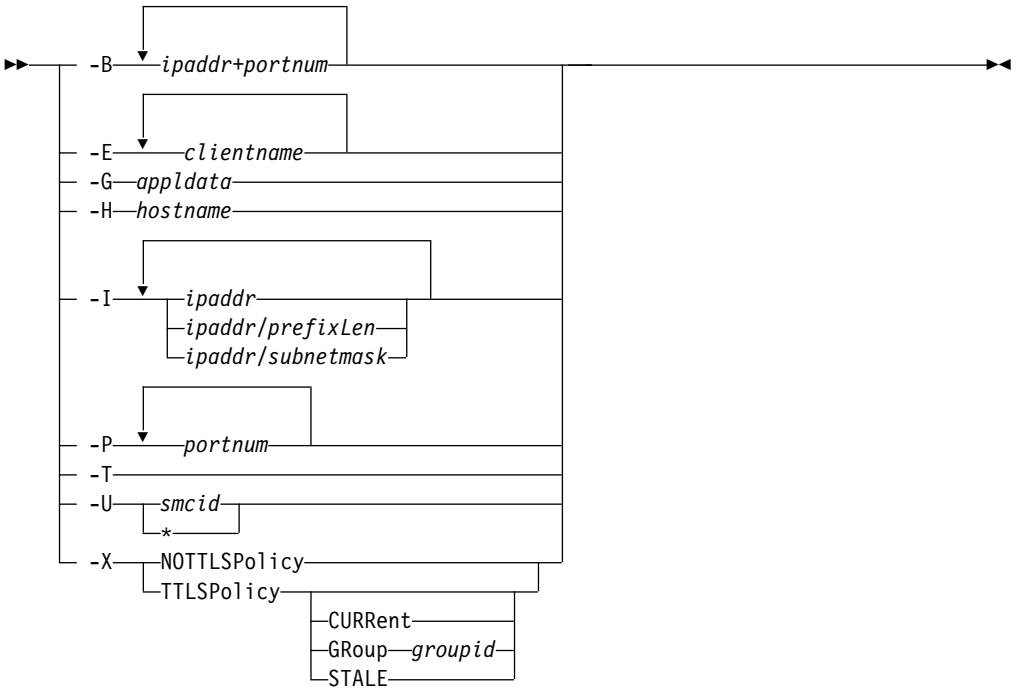
Target

Provide the report for a specific TCP/IP address space by using **-p** *tcpname*. See The Netstat command target for more information about the TCp parameter.

Output

The default output option displays the output to z/OS UNIX shell stdout. For other options, see “The z/OS UNIX netstat command syntax” on page 245 or Netstat command output.

Filter



Filter description

APPLD/-G *appldata*
Filter the output of the COnn/**-c** report using the specified application data *appldata*. You can enter one filter value at a time; the specified value can be up to 40 characters in length.

CLIent/-E *clientname*
Filter the output of the COnn/**-c** report using the specified client name *clientname*. You can enter up to six filter values; each specified value can be up to eight characters in length.

HOSTName/-H *hostname*
Filter the output of the COnn/**-c** report using the specified host name *hostname*. You can enter one filter value at a time; the specified value can be up to 255 characters in length.

Result: At the end of the report, Netstat displays the host name that the resolver used for the resolution and the list of IP addresses returned from the resolver which it used as filters.

Restrictions:

1. The HOSTName/**-H** filter does not support wildcard characters.
2. Using HOSTName/**-H** filter might cause delays in the output due to resolution of the *hostname* value depending on the resolver and DNS configuration.

IPAddr/-I *ipaddripaddr/prefixlengthipaddr/subnetmask*
Filter the report output using the specified IP address *ipaddr*, *ipaddr/prefixlength*, or *ipaddr/subnetmask*. You can enter up to six filter values; each specified IPv4 *ipaddr* value can be up to 15 characters in length.

ipaddr Filter the output of the COnn/**-c** report using the specified IP

address *ipaddr*. For IPv4 addresses, the default subnet mask of 255.255.255.255 is used. For IPv6 addresses, the default *prefixlength* value of 128 is used.

ipaddr/prefixlength
Filter the output of the COnn/**-c** report using the specified IP address and prefix length *ipaddr/prefixlength*. For a IPv4 address, the prefix length range is 1 – 32. For an IPv6 address, the prefix length range is 1 – 128.

ipaddr/subnetmask
Filter the output of the COnn/**-c** report using the specified IP address and subnet mask *ipaddr/subnetmask*. The IP address *ipaddr* in this format must be IPv4 IP address.

Guidelines:

1. The filter value *ipaddr* can be either the local or remote IP address.
2. For an IPv6 enabled stack:
   - Both IPv4 and IPv6 *ipaddr* values are accepted and can be mixed on the IPAddr/**-I** option.
   - An IPv4-mapped IPv6 address is accepted as a valid *ipaddr* value and usually provides the same result as its IPv4 address does.

Restrictions:

1. The filter value for an IPv6 address does not support wildcard characters.
2. For an IPv4-only stack, only IPv4 *ipaddr* values are accepted.
3. For a UDP endpoint socket, the filter value applies only to the local or source IP address.

IPPort/-B *ipaddr*+*portnum*
Filter the report output of the COnn/**-c** report using the specified IP address and port number. You can enter up to six filter values. Each specified IPv4 *ipaddr* value can be up to 15 characters in length, denoting a single IPv4 IP address; each specified IPv6 *ipaddr* value can be up to 45 characters in length, denoting a single IPv6 IP address. Valid *portnum* values are in the range 0 – 65535. The filter values *ipaddr* and *portnum* will match any combination of the local and remote IP address and local and remote port.

Guidelines:

- The filter value *ipaddr* can be either the local or remote IP address.
- For an IPv6-enabled stack, the following apply:
  – Both IPv4 and IPv6 *ipaddr* values are accepted and can be mixed on the IPPort/**-B** option.
  – An IPv4-mapped IPv6 address is accepted as a valid *ipaddr* value and usually provides the same result as the IPv4 address.

Restrictions:

- The *ipaddr* value in the IPPort/**-B** filter does not support wildcard characters.
- For an IPv4-only stack, only IPv4 *ipaddr* values are accepted.
- An entry is returned only when both the *ipaddr* and *portnum* values match.

- For a UDP endpoint socket, the filter value applies only to the local or source IP address and port.

NOTN3270/-T
Filter the output of the COnn/**-c** report excluding TN3270 server connections.

POrt/-P *portnum*
Filter the output of the COnn/**-c** report using the specified port number *portnum*. You can enter up to six filter values.

Guideline: The port number can be either a local or remote port.

Restriction: For a UDP endpoint socket, the filter value applies only to the local or source port.

SMCID/-U *smcid*
Filter the output of the COnn/-c report by using the specified Shared Memory Communications over Remote Direct Memory Access (SMC-R) link, SMC-R link group, or Shared Memory Communications - Direct Memory Access (SMC-D) link identifier *smcid*. If an asterisk (*) is specified for the filter value, Netstat provides output only for entries that are associated with SMC-R links, SMC-R link groups, and SMC-D links. You can enter one filter value at a time.

CONNType/-X
Filter the report using the specified connection type. You can enter one filter value at a time.

NOTTLSPolicy
Filter the output of the COnn/**-c** report, displaying only connections that have not been matched to an Application Transparent Transport Layer Security (AT-TLS) rule. This includes connections that were established while the AT-TLS function was disabled (NOTTLS was specified on the TCPCONFIG statement or in effect by default) and all connections that do not use the TCP protocol. For TCP connections that were established while the AT-TLS function was enabled, this includes:

- Connections for which AT-TLS policy lookup has not yet occurred (typically the first send or receive has not been issued yet)
- Connections for which AT-TLS policy lookup has occurred but no matching rule was found

TTLSPolicy
Filter the output of the COnn/**-c** report, displaying only connections that match an Application Transparent Transport Layer Security (AT-TLS) rule. This includes only connections that were established while the AT-TLS function was enabled, for which an AT-TLS policy rule was found with either `TTLSEnabled ON` or `TTLSEnabled OFF` specified in the TTLSGroupAction. Responses can be further limited on AT-TLS connection type. AT-TLS connection type has the following values:

CURRent
Display only connections that are using AT-TLS where the rule and all actions are still available to be used for new connections.

GRoup *groupid*
Display only connections that are using the AT-TLS group that is specified by the *groupid* value. The specified *groupid* value is a number that is assigned by the TCP/IP stack that uniquely identifies an AT-TLS group. You can determine the *groupid* value from the GroupID field value that is displayed in the Netstat TTLS/**-x** GROUP report.

STALE
Display only connections that are using AT-TLS where the rule or at least one action is no longer available to be used for new connections.

The filter value for CLIent/**-E**, IPAddr/**-I**, and APPLD/-G can be a complete string or a partial string using wildcard characters. A wildcard character can be an asterisk (*), which matches a null string or any character or character string, at the same position. A wildcard character can be a question mark (?), which matches any single character at the same position. For example, a string "searchee" matches with "*ar?he*", but the string "searhee" does not match with "*ar?he*". If you want to use the wildcard character on the IPAddr/**-I** filter, you must specify the value in the *ipaddr* format. The wildcard character is not accepted for the *ipaddr/prefixlen* or *ipaddr/subnetmask* format of IPAddr/**-I** values.

When you use z/OS UNIX **netstat**/**onetstat** command in a z/OS UNIX shell environment, take care if you use a z/OS UNIX MVS special character in a character string. It might cause an unpredictable result. To be safe, if you want to use a z/OS UNIX MVS special character in a character string, surround the character string with single (') or double (") quotation marks. For example, to use an asterisk (*) in the IP address, 10.*.0.0 for the **-I** filter, issue the command as: **netstat -c -I '10.*.0.0'** or **netstat -c -I "10.*.0.0"**.

Command syntax examples

From TSO environment

```
NETSTAT CONN
   Display information for all active TCP connections and UDP sockets in the default TCP/IP
   stack.
NETSTAT CONN TCP TCPCS6
   Display information for all active TCP connections and UDP sockets in TCPCS6 stack.
NETSTAT CONN TCP TCPCS8 (IPADDR 9.43.1.1 9.43.2.2
   Display information for these active TCP connections and UDP sockets in TCPCS8 stack
   whose local or remote IP addresses match the specified filter IP address values.
NETSTAT CONN (PORT 2222 6666 88
   Display information for those active TCP connections and UDP sockets in the default
   TCP/IP stack whose local or remote ports match the specified filter port numbers.
```

From UNIX shell environment

```
   netstat -c
   netstat -c -p tcpcs6
   netstat -c -p tcpcs6 -I 9.43.1.1 9.43.2.2
   netstat -c -P 2222 6666 88
```

Report examples

The following examples are generated by using TSO NETSTAT command. Using the z/OS UNIX **netstat** command displays the data in the same format as the TSO NETSTAT command.

Not IPv6 enabled (SHORT format)

```
NETSTAT CONN
MVS TCP/IP NETSTAT CS V2R3       TCPIP NAME: TCPCS           17:40:36
User Id  Conn     Local Socket           Foreign Socket        State
-------  ----     ------------           --------------        -----
FTPD1    0000003B 0.0.0.0..21            0.0.0.0..0            Listen
FTPD1    0000003D 9.37.65.146..21        9.67.115.5..1026      Establsh
FTPD1    0000003F 9.37.65.146..21        9.27.13.21..3711      Establsh
TCPCS    0000000F 0.0.0.0..23            0.0.0.0..0            Listen
TCPCS    0000000C 9.67.115.5..23         9.27.11.182..4886     Establsh
APPV4    00000015 0.0.0.0..2049          9.42.103.99..1234     UDP
SYSLOGD1 00000010 0.0.0.0..514           *..*                  UDP
```

IPv6 enabled or request for LONG format

```
NETSTAT CONN
MVS TCP/IP NETSTAT CS V2R3       TCPIP NAME: TCPCS           17:40:36
User Id  Conn     State
-------  ----     -----
FTPD1    0000004A Listen
  Local Socket:   ::..21
  Foreign Socket: ::..0
FTPD1    00000052 Establsh
  Local Socket:   ::ffff:9.67.115.5..21
  Foreign Socket: ::ffff:9.67.115.65..1026
FTPD1    00000058 Establsh
  Local Socket:   2001:0db8::9:67:115:66..21
  Foreign Socket: 2001:0db8::9:67:115:65..1027
TCPCS    0000001A Listen
  Local Socket:   0.0.0.0..23
  Foreign Socket: 0.0.0.0..0
TCPCS    0000001E Establsh
  Local Socket:   9.67.115.5..23
  Foreign Socket: 9.27.11.182..4665
USER3    0000005F Establsh
  Local Socket:   2001:0db8::9:67:115:5..1079
  Foreign Socket: 2001:0db8::9:67:115:65..21
USER6    000000C7 Establsh
  Local Socket:   9.67.115.5..1027
  Foreign Socket: 9.37.65.146..21
APPM     00000017 UDP
  Local Socket:   ::ffff.0.0.0.0..2051
  Foreign Socket: ::ffff.9.42.103.99..1234
APPV4    00000015 UDP
  Local Socket:   0.0.0.0..2049
  Foreign Socket: 9.42.103.99..1234

SYSLOGD1 0000002C UDP
  Local Socket:   0.0.0.0..529
  Foreign Socket: *..*
```

Report field descriptions

User Id
See the Client name or User ID information in Netstat report general concepts for a detailed description.

Conn See the Client ID or Connection Number information in Netstat report general concepts for a detailed description.

Local Socket
See the Local Socket information in Netstat report general concepts for a detailed description.

Foreign Socket
See the Foreign Socket information in Netstat report general concepts for a detailed description.

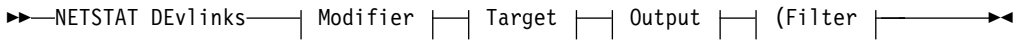
State See the TCP connection status and UDP socket status information in Netstat report general concepts for a detailed description.

Application Data
The application data that makes it easy for you to locate and display the connections that are used by the application. The beginning of the application data identifies the format of the application data area. For z/OS Communications Server applications, see application data in the z/OS Communications Server: IP Programmer's Guide and Reference for a description of the format, content, and meaning of the data that is supplied by the application. For other applications, see the documentation that is supplied by the application. The data is displayed in character format if application data is present. Non-printable characters, if any, are displayed as dots.

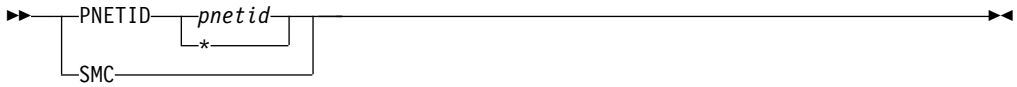
Netstat DEvlinks/-d report

Displays information about interfaces that are defined to the TCP/IP stack.

TSO syntax



Modifier



PNETID=*pnetid*
Displays information about interfaces for the specified physical network ID (*pnetid*). If an asterisk (*) is specified for the PNETID value, all interfaces with a PNETID value are displayed. This modifier is mutually exclusive with the SMC modifier.

SMC Displays only Shared Memory Communications (SMC) information.

- For Shared Memory Communications over Remote Direct Memory Access (SMC-R), the information is about 10GbE RoCE Express interfaces and their associated SMC-R link groups and SMC-R links.
- For Shared Memory Communications - Direct Memory Access (SMC-D), the information is about Internal Shared Memory (ISM) interfaces and their associated SMC-D links.

This modifier is mutually exclusive with the PNETID modifier.

Tip: If the INTFName/-K filter is specified with the SMC modifier, the SMC-R link group information is not displayed.

Target

Provide the report for a specific TCP/IP address space by using TCp *tcpname*. See The Netstat command target for more information about the TCp parameter.

Output

The default output option displays the output on the user's terminal. For other options, see "The TSO NETSTAT command syntax" on page 241 or Netstat command output.

Filter

z/OS UNIX syntax

Modifier

PNETID=*pnetid*
Displays information about interfaces for the specified physical network ID (*pnetid*). If an asterisk (*) is specified for the PNETID value, all interfaces with a PNETID value are displayed. This modifier is mutually exclusive with the SMC modifier.

SMC Provide only Shared Memory Communications (SMC) information.

- For Shared Memory Communications over Remote Direct Memory Access (SMC-R), the information is about 10GbE RoCE Express® interfaces and their associated SMC-R link groups and SMC-R links.
- For Shared Memory Communications - Direct Memory Access (SMC-D), the information is about Internal Shared Memory (ISM) interfaces and their associated SMC-D links.

This modifier is mutually exclusive with the PNETID modifier.

Tip: If the INTFName/-K filter is specified with the SMC modifier, the SMC-R link group information is not displayed.

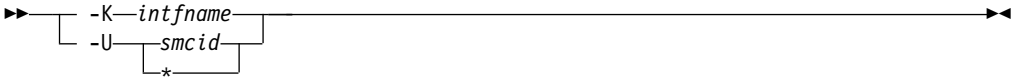
Target

Provide the report for a specific TCP/IP address space by using **-p** *tcpname*. See The Netstat command target for more information about the TCp parameter.

Output

The default output option displays the output to z/OS UNIX shell stdout. For other options, see "The z/OS UNIX netstat command syntax" on page 245 or Netstat command output.

Filter



Filter description

INTFName/-K *intfname*

Filter the output of the DEvlinks/**-d** report using the specified interface name *intfname*. You can enter one filter value at a time and the specified value can be up to 16 characters in length.

The INTFName/**-K** filter value *intfname* can be one of the following values:

- The network interface name that was displayed in the LnkName/LinkName or INTFName field in the report (this option selects one interface).
- The interface name of an OSAENTA trace interface, which is EZANTA*portname*, where the *portname* value is the name that is specified on the PORTNAME keyword in the TRLE for the OSA-Express port that is being traced (this option selects one interface).
- The port name of an OSA-Express feature in QDIO mode, where the port name is the name that is specified on the PORTNAME keyword in the TRLE (this option selects all interfaces that are associated with the OSA-Express port, including an OSAENTA trace interface).
- The name of a HiperSockets TRLE. This option selects all interfaces that are associated with the HiperSockets TRLE.

Restriction:

- The INTFName/**-K** filter value does not support wildcard characters.
- The INTFName/**-K** filter value does not display information for a device that does not have a link defined.
- The INTFName/**-K** filter is not supported for the report if the PNETID modifier is specified.

SMCID/-U *smcid*

Filter the output of the DEvlinks/-d report by using the specified Shared Memory Communications over Remote Direct Memory Access (SMC-R) link, SMC-R link group, or Shared Memory Communications - Direct Memory Access (SMC-D) link identifier *smcid*. You can enter one filter value at a time.

- If the filter value is an SMC-R link ID, then the report shows details about that SMC-R link and information about the SMC-R link group to which that link belongs.
- If the filter value is an SMC-R link group ID, then the report shows details about all SMC-R links in the link group and information about the SMC-R link group.
- If the filter value is an SMC-D link ID, then the report shows details about that SMC-D link.
- If the filter value is an asterisk (*), then the report provides the same information that the SMC modifier provides.

Rule: If you specify the SMCID/-U filter on the command, the report is generated as if the SMC modifier was also specified. The report includes detailed information about the SMC-R link or SMC-D link that *smcid* defines, regardless of whether the SMC modifier was explicitly coded. Using the SMCID/-U filter with the filter value asterisk (*) is equivalent to using the SMC modifier. The SMCID/-U filter is not supported for the report if the PNETID modifier is specified.

Command syntax examples

From TSO environment

```
NETSTAT DEVLINKS
   Displays the information about devices and defined interfaces or links in the default
   TCP/IP address space
NETSTAT DEVLINKS TCP TCPCS6
   Displays the information about devices and defined interfaces or links in the TCPCS6
   TCP/IP address space.
NETSTAT DEVLINKS SMC
   Displays additional SMC-D information about ISM interfaces, and SMC-R information about
RNIC interfaces.
NETSTAT DEVLINKS PNETID NETID1
   Displays the information about interfaces with a PNETID value of NETID1.
NETSTAT DEVLINKS TCP TCPCS8 (INTFNAME OSAQDIOLINK
   Display the information for the OSAQDIOLINK in the TCPCS8 TCP/IP adress space.
```

From UNIX shell environment

```
   netstat -d
   netstat -d -p tcpcs6
   netstat -d SMC
   netstat -d PNETID NETID1
   netstat -d -p tcpcs8 -K OSAQDIOLINK
```

Report examples

The following examples are generated by using TSO NETSTAT command. Using the z/OS UNIX **netstat** command displays the data in the same format as the TSO NETSTAT command.

Not IPv6 enabled (SHORT format)

```
NETSTAT DEVLINKS MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           14:23:39
DevName: LOOPBACK          DevType: LOOPBACK
  DevStatus: Ready
  LnkName: LOOPBACK          LnkType: LOOPBACK   LnkStatus: Ready
    ActMtu: 65535
  Routing Parameters:
    MTU Size: n/a               Metric: 00
    DestAddr: 0.0.0.0           SubnetMask: 0.0.0.0
  Multicast Specific:
    Multicast Capability: No
  Link Statistics:
    BytesIn                           = 24943
    Inbound Packets                   = 100
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 24943
    Outbound Packets                  = 100
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0

DevName: LCS1              DevType: LCS       DevNum: 0D00
  DevStatus: Ready
  LnkName: TR1               LnkType: TR          LnkStatus: Ready
    NetNum: 0    QueSize: 0
    MacAddrOrder: Non-Canonical    SrBridgingCapability: Yes
    IpBroadcastCapability: Yes     ArpBroadcastType: All Rings
    MacAddress: 08005A0D97A2
    ActMtu: 1492
    SecClass: 8                      MonSysplex: Yes
  Routing Parameters:
    MTU Size: 02000             Metric: 100
    DestAddr: 0.0.0.0           SubnetMask: 255.255.255.128
  Packet Trace Setting:
    Protocol: *                 TrRecCnt: 00000006  PckLength: FULL
    Discard : NONE
    SrcPort: *                  DestPort: *         PortNum: *
    IpAddr: *                   SubNet: *
```

```
  Multicast Specific:
    Multicast Capability: Yes
    Group             RefCnt      SrcFltMd
    -----             ------      --------
    224.0.0.1         0000000001  Include
      SrcAddr: 9.1.1.1
               9.1.1.2
               9.1.1.3
    224.9.9.3         0000000001  Include
      SrcAddr: 9.1.1.1
    224.9.9.4         0000000001  Exclude
      SrcAddr: 9.2.2.1
               9.2.2.2
    225.9.9.4         0000000003  Exclude
      SrcAddr: None
  Link Statistics:
    BytesIn                           = 9130
    Inbound Packets                   = 2
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 60392
    Outbound Packets                  = 11
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0

DevName: OSAQDIO4          DevType: MPCIPA
  DevStatus: Ready         CfgRouter: Non  ActRouter: Non
  LnkName: OSAQDIOLINK       LnkType: IPAQENET   LnkStatus: Ready
    Speed: 0000000100
    IpBroadcastCapability: No
    VMACAddr:   000629DC21BC  VMACOrigin: Cfg  VMACRouter: All
    ArpOffload: Yes                   ArpOffloadInfo: Yes
    ActMtu: 1492
    VLANid: 1260                      VLANpriority: Enabled
    DynVLANRegCfg: Yes                DynVLANRegCap: No
    ReadStorage: GLOBAL (8064K)       InbPerf: Balanced
    ReadStorage: GLOBAL (8064K)
    InbPerf: Balanced
    ChecksumOffload: Yes              SegmentationOffload: Yes
    SecClass: 8                       MonSysplex: Yes
  Routing Parameters:
    MTU Size: n/a               Metric: 00
    DestAddr: 0.0.0.0           SubnetMask: 255.255.255.192
  Multicast Specific:
    Multicast Capability: Yes
    Group             RefCnt        SrcFltMd
    -----             ------        --------
    224.0.0.1         0000000001    Exclude
      SrcAddr: None
  Link Statistics:
    BytesIn                           = 11476
    Inbound Packets                   = 10
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 6707
    Outbound Packets                  = 10
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0
```

```
DevName: OSATRL90          DevType: ATM
  DevStatus: Not Active
  LnkName: OSA90LINK1        LnkType: ATM         LnkStatus: Not Active
    ActMtu: Unknown
    SecClass: 8                      MonSysplex: Yes
  Routing Parameters:
    MTU Size: n/a               Metric: 00
    DestAddr: 0.0.0.0           SubnetMask: 255.0.0.0
  ATM Specific:
    ATM portName:  OSA90
    ATM PVC Name:  STEPH             PVC Status: Not Active

    ATM LIS Name:  LIS1
    SubnetValue:   9.67.1.0          SubnetMask:    255.255.255.0
    DefaultMTU:    0000009180        InactvTimeOut: 0000000300
    MinHoldTime:   0000000060        MaxCalls:      0000001000
    CachEntryAge:  0000000900        ATMArpReTry:   0000000002
    ATMArpTimeOut: 0000000003        PeakCellRate:  0000000000
    NumOfSVCs:     0000000000        BearerClass:   C

    ATMARPSV Name: ARPSV1
    VcType:        PVC               ATMaddrType: NSAP
    ATMaddr:
    IpAddr:        0.0.0.0
  Multicast Specific:
    Multicast Capability: No
  Link Statistics:
    BytesIn                          = 0
    Inbound Packets                  = 0
    Inbound Packets In Error         = 0
    Inbound Packets Discarded        = 0
    Inbound Packets With No Protocol = 0
    BytesOut                         = 0
    Outbound Packets                 = 0
    Outbound Packets In Error        = 0
    Outbound Packets Discarded       = 0

DevName: CLAW2             DevType: CLAW      DevNum: 0D10
  DevStatus: Ready         CfgPacking: Packed ActPacking: Packed
  LnkName: CLAW2LINK         LnkType: CLAW        LnkStatus: Ready
    ActMtu: 2600
    SecClass: 8                      MonSysplex: No
  Routing Parameters:
    MTU Size: n/a               Metric: 00
    DestAddr: 0.0.0.0           SubnetMask: 255.255.255.0
  Multicast Specific:
    Multicast Capability: No
  Link Statistics:
    BytesIn                          = 0
    Inbound Packets                  = 0
    Inbound Packets In Error         = 0
    Inbound Packets Discarded        = 0
    Inbound Packets With No Protocol = 0
    BytesOut                         = 0
    Outbound Packets                 = 0
    Outbound Packets In Error        = 0
    Outbound Packets Discarded       = 0
```

```
DevName: IUTIQDIO          DevType: MPCIPA
  DevStatus: Ready
  LnkName: IQDIOLNK0A3D0001  LnkType: IPAQIDIO   LnkStatus: Ready
    IpBroadcastCapability: No
    CfgRouter: Non                   ActRouter: Non
    ArpOffload: Yes                  ArpOffloadInfo: No
    ActMtu: 8192
    ReadStorage: GLOBAL (2048K)
    SecClass: 255
    IQDMultiWrite: Enabled
  Routing Parameters:
    MTU Size: 8192              Metric: 00
    DestAddr: 0.0.0.0           SubnetMask: 255.255.0.0
  Multicast Specific:
    Multicast Capability: Yes
    Group             RefCnt        SrcFltMd
    -----             ------        --------
    224.0.0.1         0000000001    Exclude
      SrcAddr: None
  Link Statistics:
    BytesIn                           = 0
    Inbound Packets                   = 0
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 0
    Outbound Packets                  = 0
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0

IntfName: OSAQDIOINTF       IntfType: IPAQENET   IntfStatus: Ready
    PortName: OSAQDIO2  Datapath: 0E2A     DatapathStatus: Ready
    CHPIDType: OSD   SMCR: Yes
    PNetID: NETWORK3          SMCD : Yes
    Speed: 0000000100
    IpBroadcastCapability: No
    VMACAddr:   020629DC21BD  VMACOrigin: Cfg  VMACRouter: All
    SrcVipaIntf: VIPAV4
    CfgRouter: Non                   ActRouter: Non
    ArpOffload: Yes                  ArpOffloadInfo: Yes
    CfgMtu: 1492                     ActMtu: 1492
    IpAddr: 100.1.1.1/24
    VLANid: 1261                     VLANpriority: Enabled
    DynVLANRegCfg: Yes               DynVLANRegCap: No
    ReadStorage: GLOBAL (8064K)      InbPerf: Balanced
    ReadStorage: GLOBAL (8064K)
    InbPerf: Dynamic
      WorkloadQueueing: Yes
    ChecksumOffload: Yes             SegmentationOffload: Yes
    SecClass: 9                      MonSysplex: Yes
    Isolate: Yes                     OptLatencyMode: Yes
  Multicast Specific:
    Multicast Capability: Yes
    Group             RefCnt        SrcFltMd
    -----             ------        --------
    224.0.0.1         0000000001    Exclude
  SrcAddr: None
  Interface Statistics:
    BytesIn                           = 12834
    Inbound Packets                   = 16
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 5132
    Outbound Packets                  = 10
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0
  Associated RNIC interface: EZARIUT10005
  Associated RNIC interface: EZARIUT10006
  Associated ISM interface: EZAISM02
```

```
IntfName: IQDINTF1          IntfType: IPAQIDIO   IntfStatus: Ready
    TRLE: IUTIQ4QD  Datapath: 0E2A     DatapathStatus: Ready
    CHPID: D1
    PNetID: PHYSICALNETWORK2    SMCD: Yes
    IpBroadcastCapability: No
    SrcVipaIntf: VIPAV4
    ArpOffload: Yes                  ArpOffloadInfo: No
    CfgMtu: 8192                     ActMtu: 8192
    IpAddr: 100.1.1.1/24
    VLANid: 1261
    ReadStorage: GLOBAL (2048K)
    SecClass: 255
    IQDMultiWrite: Enabled
  Multicast Specific:
    Multicast Capability: Yes
    Group             RefCnt        SrcFltMd
    -----             ------        --------
    224.0.0.1         0000000001    Exclude
      SrcAddr: None
  Interface Statistics:
    BytesIn                           = 0
    Inbound Packets                   = 0
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 0
    Outbound Packets                  = 0
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0
  Associated ISM interface: EZAISM01

IntfName: VDEV1             IntfType: VIPA       IntfStatus: Ready
    IpAddr: 100.1.1.1/24
  Multicast Specific:
    Multicast Capability: No
```

```
IntfName: OSXC9INT1         IntfType: IPAQENET   IntfStatus: Ready
    PortName: IUTXP0C9  Datapath: 0E56     DatapathStatus: Ready
    CHPIDType: OSX      CHPID: C9
    PNetID: IEDN
    Speed: 0000001000
    IpBroadcastCapability: No
    VMACAddr: 420001AA0E56  VMACOrigin: OSA  VMACRouter: All
    CfgRouter: Non                 ActRouter: Non
    ArpOffload: Yes                ArpOffloadInfo: No
    CfgMtu: None                   ActMtu: 8992
    IpAddr: 172.16.0.1/16
    VLANid: 401                    VLANpriority: Disabled
    DynVLANRegCfg: No              DynVLANRegCap: Yes
    ReadStorage: GLOBAL (512K)
    InbPerf: Dynamic
      WorkloadQueueing: No
    ChecksumOffload: No            SegmentationOffload: No
    SecClass: 255                  MonSysplex: No
    Isolate: No                    OptLatencyMode: No
  Multicast Specific:
    Multicast Capability: Yes
    Group             RefCnt      SrcFltMd
    -----             ------      --------
    224.0.0.1         0000000001  Exclude
      SrcAddr: None
  Interface Statistics:
    BytesIn                          = 0
    Inbound Packets                  = 0
    Inbound Packets In Error         = 0
    Inbound Packets Discarded        = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                         = 0
    Outbound Packets                 = 0
    Outbound Packets In Error        = 0
    Outbound Packets Discarded       = 0
  Associated IQDX interface: EZAIQXC9  IQDX Status: Ready
    BytesIn                          = 0
    Inbound Packets                  = 0
    BytesOut                         = 0
    Outbound Packets                 = 0


IntfName: EZAIQXC9          IntfType: IPAQIQDX    IntfStatus: Ready
    Datapath: 0E0E     DatapathStatus: Ready
    VMACAddr: 820001AA0E0E
    ReadStorage: MAX (2048K)
    IQDMultiWrite: Disabled
  Multicast Specific:
    Multicast Capability: No
  Interface Statistics:
    BytesIn                          = 0
    Inbound Packets                  = 0
    Inbound Packets In Error         = 0
    Inbound Packets Discarded        = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                         = 0
    Outbound Packets                 = 0
    Outbound Packets In Error        = 0
    Outbound Packets Discarded       = 0
```

```
IntfName: EZARIUT10005      IntfType: RNIC       IntfStatus: Ready
  PFID: 0005  PortNum: 1  TRLE: IUT10005
  PNetID: NETWORK3
  VMACAddr: 02000012F030
  GIDAddr:  fe80::200:ff:fe12:f030
  Interface Statistics:
    BytesIn                          = 18994
    Inbound Operations               = 146
    BytesOut                         = 19139
    Outbound Operations              = 811
    SMC Links                        = 2
    TCP Connections                  = 1
    Intf Receive Buffer Inuse        = 64K
IntfName: EZARIUT10006      IntfType: RNIC       IntfStatus: Ready
  PFID: 0006  PortNum: 1  TRLE: IUT10006
  PNetID: NETWORK3
  VMACAddr: 02000012EF50
  GIDAddr:  fe80::200:ff:fe12:ef50
  Interface Statistics:
    BytesIn                          = 226
    Inbound Operations               = 4
    BytesOut                         = 29
    Outbound Operations              = 4
    SMC Links                        = 2
    TCP Connections                  = 1
    Intf Receive Buffer Inuse        = 64K

IntfName: EZAISM01      IntfType: ISM       IntfStatus: Ready
  PFID: 0061  TRLE: IUT00061  PFIDStatues: Ready
  PNetID: PHYSICALNETWORK2
  GIDAddr:  8002000900090061
  Interface Statistics:
    BytesIn                          = 0
    Inbound Operations               = 0
    BytesOut                         = 0
    Outbound Operations              = 0
    SMC Links                        = 0
    TCP Connections                  = 0
    Intf Receive Buffer Inuse        = 0K
    Device Interrupts                = 0
IPv4 LAN Group Summary
 LanGroup: 001

   Name              Status      ArpOwner          VipaOwner
   -------           ------      --------          ---------
   OSXC9INT1         Active      OSXC9INT1         Yes
   TR1               Active      TR1               No

 LanGroup: 002

   Name              Status      ArpOwner          VipaOwner
   -------           ------      --------          ---------
   OSAQDIOLINK       Active      OSAQDIOLINK       Yes
   OSAQDIOINTF       Active      OSAQDIOINTF       No
```

```
Netstat DEvlinks/-d PNETID *
MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS1          12:17:36
PNetID: PHYSICALNETWORK2
  IntfName: IQDIOLNK0A3D0001  IntfType: IPAQIDIO
  IntfName: EZAISM01          IntfType: ISM        Associated: Yes
PNetID: NETID1
  IntfName: QDIO4SHRL         IntfType: IPAQENET
  IntfName: EZAISM02          IntfType: ISM        Associated: Yes
  IntfName: EZARIUT1A003      IntfType: RNIC       Associated: Yes
  IntfName: EZARIUT1A004      IntfType: RNIC       Associated: Yes
```

```
Netstat DEvlinks/-d PNETID NETID1
MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS1          12:29:32
IntfName: QDIO4SHRL         IntfType: IPAQENET
  TRLE: QDIO001   CHPID: C7   PChid: 01C7  CHPIDType: OSD
  PortName: QDIO4SHR          SMCR:  Yes
  Datapath: 0E42  VLANid: None  SMCD: Yes

IntfName: EZAISM02          IntfType: ISM        Associated: Yes
  TRLE: IUT00051  PFID: 0051  VChid: 2300
  GIDAddr: 8002000100010051

IntfName: EZARIUT1A004      IntfType: RNIC       Associated: Yes
  TRLE: IUT1A004  PFID: A004  PChid: 0120  PortNum: 1
  VMACAddr: D4C1C301A004
  GIDAddr: fe80::d4c1:c301:a004

IntfName: EZARIUT1A003      IntfType: RNIC       Associated: Yes
  TRLE: IUT1A003  PFID: A003  PChid: 0118  PortNum: 1
  VMACAddr: D4C1C301A003
  GIDAddr: fe80::d4c1:c301:a003
```

IPv6 enabled or request for LONG format

```
NETSTAT DEVLINKS
MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           14:23:39
DevName: LOOPBACK          DevType: LOOPBACK
  DevStatus: Ready
  LnkName: LOOPBACK          LnkType: LOOPBACK   LnkStatus: Ready
    ActMtu: 65535
  Routing Parameters:
    MTU Size: n/a               Metric: 00
    DestAddr: 0.0.0.0           SubnetMask: 0.0.0.0
  Multicast Specific:
    Multicast Capability: No
  Link Statistics:
    BytesIn                          = 7665
    Inbound Packets                  = 100
    Inbound Packets In Error         = 0
    Inbound Packets Discarded        = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                         = 7665
    Outbound Packets                 = 100
    Outbound Packets In Error        = 0
    Outbound Packets Discarded       = 0

IntfName: LOOPBACK6        IntfType: LOOPBACK6 IntfStatus: Ready
    ActMtu: 65535
  Multicast Specific:
    Multicast Capability: No
  Interface Statistics:
    BytesIn                          = 0
    Inbound Packets                  = 0
    Inbound Packets In Error         = 0
    Inbound Packets Discarded        = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                         = 0
    Outbound Packets                 = 0
    Outbound Packets In Error        = 0
    Outbound Packets Discarded       = 0

DevName: LCS1              DevType: LCS       DevNum: 0D00
  DevStatus: Ready
  LnkName: TR1               LnkType: TR          LnkStatus: Ready
    NetNum: 0    QueSize: 0
    MacAddrOrder: Non-Canonical    SrBridgingCapability: Yes
    IpBroadcastCapability: Yes     ArpBroadcastType: All Rings
    MacAddress: 08005A0D97A2
    ActMtu: 1492
    SecClass: 8                      MonSysplex: Yes
  Routing Parameters:
    MTU Size: 02000             Metric: 100
    DestAddr: 0.0.0.0           SubnetMask: 255.255.255.128
  Packet Trace Setting:
    Protocol: *                 TrRecCnt: 00000006  PckLength: FULL
    Discard : NONE
    SrcPort: *                  DestPort: *         PortNum: *
    IpAddr: *                   SubNet: *
```

```
  Multicast Specific:
    Multicast Capability: Yes
    Group             RefCnt      SrcFltMd
    -----             ------      --------
    224.9.9.1         0000000002  Include
      SrcAddr: 9.1.1.1
               9.1.1.2
               9.1.1.3
    224.9.9.3         0000000001  Include
      SrcAddr: 9.1.1.1
    224.9.9.4         0000000001  Exclude
      SrcAddr: 9.2.2.1
               9.2.2.2
    225.9.9.4         0000000003  Exclude
      SrcAddr: None
  Link Statistics:
    BytesIn                           = 9130
    Inbound Packets                   = 2
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 60392
    Outbound Packets                  = 11
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0

DevName: OSAQDIO4          DevType: MPCIPA
  DevStatus: Ready
  LnkName: OSAQDIOLINK       LnkType: IPAQENET   LnkStatus: Ready
    Speed: 0000000100
    IpBroadcastCapability: No
    VMACAddr:   000629DC21BC  VMACOrigin: Cfg  VMACRouter: All
    CfgRouter: Non                    ActRouter: Non
    ArpOffload: Yes                   ArpOffloadInfo: Yes
    ActMtu: 1492
    VLANid: 1260                      VLANpriority: Enabled
    DynVLANRegCfg: Yes                DynVLANRegCap: No
    ReadStorage: GLOBAL (8064K)       InbPerf: Balanced
    ReadStorage: GLOBAL (8064K)
    InbPerf: Balanced
    ChecksumOffload: Yes              SegmentationOffload: Yes
    SecClass: 8                       MonSysplex: Yes
  Routing Parameters:
    MTU Size: n/a               Metric: 00
    DestAddr: 0.0.0.0           SubnetMask: 255.255.255.192
  Multicast Specific:
    Multicast Capability: Yes
    Group             RefCnt        SrcFltMd
    -----             ------        --------
    224.0.0.1         0000000001    Exclude
      SrcAddr: None
  Link Statistics:
    BytesIn                           = 11476
    Inbound Packets                   = 10
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 6707
    Outbound Packets                  = 10
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0
```

```
IntfName: OSAQDIO46        IntfType: IPAQENET6   IntfStatus: Ready
    PortName: OSAQDIO4  Datapath: 0E2B     DatapathStatus: Ready
    CHPIDType: OSD      SMCR: Yes
    PNetID: NETWORK3    SMCD : Yes
    QueSize: 0  Speed: 0000000100
    VMACAddr:   000629DC21BC  VMACOrigin: Cfg  VMACRouter: All
    SrcVipaIntf: VIPAV6
    DupAddrDet: 1
    CfgRouter: Pri                   ActRouter: Pri
    RtrHopLimit: 5
    CfgMtu: 4096                     ActMtu: 1492
    VLANid: 1261                     VLANpriority: Enabled
    DynVLANRegCfg: Yes               DynVLANRegCap: No
    IntfID: 0000:0000:0000:0001
    ReadStorage: GLOBAL (8064K)
    InbPerf: Balanced
    ChecksumOffload: Yes             SegmentationOffload: Yes
    SecClass: 8                      MonSysplex: Yes
    Isolate: Yes                     OptLatencyMode: Yes
    TempPrefix: 2001:0db8:3454:a3cf::/64
                2001:0db8:58cd::/48

  Packet Trace Setting:
    Protocol: *                 TrRecCnt: 00000000  PckLength: FULL
    SrcPort:  *                 DestPort: *
    IpAddr/PrefixLen: 9::44/128
  Multicast Specific:
    Multicast Capability: Yes
    Group:     ff02::1:ff15:5
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: 2e00::11
               2e00::22
    Group:     ff02::1:ffdc:217c
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
    Group:     ff02::1
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
    Group:     ff02::1:ff00:2
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
  Interface Statistics:
    BytesIn                           = 12655
    Inbound Packets                   = 12
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 4590
    Outbound Packets                  = 11
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0
  Associated RNIC interface: EZARIUT10005
  Associated RNIC interface: EZARIUT10006
```

```
IntfName: V6SAMEH          IntfType: MPCPTP6   IntfStatus: Not Active
    TRLE: IUTSAMEH   DevStatus: Not Active
    SrcVipaIntf: VIPAV6
    ActMtu: Unknown
    IntfID: 0000:0000:0000:0001
    SecClass: 8
  Multicast Specific:
    Multicast Capability: No
  Interface Statistics:
    BytesIn                          = 0
    Inbound Packets                  = 0
    Inbound Packets In Error         = 0
    Inbound Packets Discarded        = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                         = 0
    Outbound Packets                 = 0
    Outbound Packets In Error        = 0

IntfName: VIPAV6           IntfType: VIPA6     IntfStatus: Ready
  Packet Trace Setting:
    Protocol: *                TrRecCnt: 00000000  PckLength: FULL
    SrcPort:  *                DestPort: *         PortNum: *
    IpAddr:   *                SubNet:   *
  Multicast Specific:
    Multicast Capability: No
```

```
IntfName: SZQIDIO6          IntfType: IPAQIDIO6  IntfStatus: Not Active
    TRLE: IUTIQDD1  Datapath: 0E3A     DatapathStatus: Not Active
    CHPID: D1
    PNetID: PHYSICALNETWORK2    SMCD: Yes
    ActMtu: Unknown
    VLANid: 3
    SecClass: 044                    MonSysplex: No
  Multicast Specific:
    Multicast Capability: Unknown
    Group:     ff02::1:ff00:2
      RefCnt:  0000000002  SrcFltMd: Exclude
      SrcAddr: None
  Interface Statistics:
    BytesIn                          = 0
    Inbound Packets                  = 0
    Inbound Packets In Error         = 0
    Inbound Packets Discarded        = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                         = 0
    Outbound Packets                 = 0
    Outbound Packets In Error        = 0
  Associated ISM interface: EZAISM01
```

```
IntfName: OSAQDIOINTF       IntfType: IPAQENET   IntfStatus: Ready
    PortName: OSAQDIO2  Datapath: 0E2A     DatapathStatus: Ready
    CHPIDType: OSD         SMCR: Yes
    PNetID: ZOSNET         SMCD: Yes
    Speed: 0000000100
    IpBroadcastCapability: No
    VMACAddr:   020629DC21BD  VMACOrigin: Cfg  VMACRouter: All
    SrcVipaIntf: VIPAV4
    CfgRouter: Non                    ActRouter: Non
    ArpOffload: Yes                   ArpOffloadInfo: Yes
    CfgMtu: 1492                      ActMtu: 1492
    IpAddr: 100.1.1.1/24
    VLANid: 1261                      VLANpriority: Enabled
    DynVLANRegCfg: Yes                DynVLANRegCap: No
    ReadStorage: GLOBAL (8064K)
    InbPerf: Balanced
    ChecksumOffload: Yes              SegmentationOffload: Yes
    SecClass: 9                       MonSysplex: Yes
    Isolate: Yes
  Multicast Specific:
    Multicast Capability: Yes
    Group             RefCnt        SrcFltMd
    -----             ------        --------
    224.0.0.1         0000000001    Exclude
      SrcAddr: None
  Interface Statistics:
    BytesIn                           = 12834
    Inbound Packets                   = 16
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 5132
    Outbound Packets                  = 10
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0
  Associated RNIC interface: EZARIUT10005
  Associated RNIC interface: EZARIUT10006
  Associated ISM interface: EZAISM02
```

```
IntfName: OSXC9INT2         IntfType: IPAQENET6  IntfStatus: Ready
    PortName: IUTXP0C9  Datapath: 0E56     DatapathStatus: Ready
    CHPIDType: OSX      CHPID: C9
    PNetID: IEDN
    QueSize: 0    Speed: 0000001000
    VMACAddr: 620001AA0E56   VMACOrigin: OSA    VMACRouter: All
    DupAddrDet: 1
    CfgMtu: None                      ActMtu: 9000
    VLANid: 602                       VLANpriority: Disabled
    DynVLANRegCfg: No                 DynVLANRegCap: Yes
    ReadStorage: GLOBAL (512K)
    InbPerf: Dynamic
      WorkloadQueueing: No
    ChecksumOffload: No               SegmentationOffload: No
    SecClass: 255                     MonSysplex: No
    Isolate: No                       OptLatencyMode: No
    TempPrefix: All
  Multicast Specific:
    Multicast Capability: Yes
    Group:     ff02::1:ffaa:e56
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
    Group:     ff01::1
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
    Group:     ff02::1
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
    Group:     ff02::1:ff01:1
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
    Group:     ff02::1:ff00:2
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
    Group:     ff02::1:ff00:1
      RefCnt:  0000000002  SrcFltMd: Exclude
      SrcAddr: None
  Interface Statistics:
    BytesIn                           = 0
    Inbound Packets                   = 0
    Inbound Packets In Error          = 0
    Inbound Packets Discarded         = 0
    Inbound Packets With No Protocol  = 0
    BytesOut                          = 688
    Outbound Packets                  = 7
    Outbound Packets In Error         = 0
    Outbound Packets Discarded        = 0
  Associated IQDX interface: EZ6IQXC9  IQDX Status: Ready
    BytesIn                           = 0
    Inbound Packets                   = 0
    BytesOut                          = 0
    Outbound Packets                  = 0
```

```
IntfName: EZ6IQXC9          IntfType: IPAQIQDX6   IntfStatus: Ready
    Datapath: 0E0E          DatapathStatus: Ready
    VMACAddr: 820001AA0E0E
    ReadStorage: MAX (2048K)
    IQDMultiWrite: Disabled
  Multicast Specific:
    Multicast Capability: ND only
    Group:     ff02::1:ffaa:e56
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
    Group:     ff02::1:ff01:1
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
    Group:     ff02::1:ff00:2
      RefCnt:  0000000001  SrcFltMd: Exclude
      SrcAddr: None
    Group:     ff02::1:ff00:1
      RefCnt:  0000000002  SrcFltMd: Exclude
      SrcAddr: None
  Interface Statistics:
    BytesIn                          = 0
    Inbound Packets                  = 0
    Inbound Packets In Error         = 0
    Inbound Packets Discarded        = 0
    Inbound Packets With No Protocol = 0
    BytesOut                         = 0
    Outbound Packets                 = 0
    Outbound Packets In Error        = 0
    Outbound Packets Discarded       = 0


IntfName: EZARIUT10005      IntfType: RNIC       IntfStatus: Ready
  PFID: 0005  PortNum: 1  TRLE: IUT10005 PFIDStatus: Ready
  PNetID: NETWORK3
  VMACAddr: 02000012F030
  GIDAddr:  fe80::200:ff:fe12:f030
  Interface Statistics:
    BytesIn                          = 18994
    Inbound Operations               = 146
    BytesOut                         = 19139
    Outbound Operations              = 811
    SMC Links                        = 2
    TCP Connections                  = 1
    Intf Receive Buffer Inuse        = 64K

IntfName: EZARIUT10006      IntfType: RNIC       IntfStatus: Ready
  PFID: 0006  PortNum: 1  TRLE: IUT10006 PFIDStatus: Ready
  PNetID: NETWORK3
  VMACAddr: 02000012EF50
  GIDAddr:  fe80::200:ff:fe12:ef50
  Interface Statistics:
    BytesIn                          = 226
    Inbound Operations               = 4
    BytesOut                         = 29
    Outbound Operations              = 4
    SMC Links                        = 2
    TCP Connections                  = 1
    Intf Receive Buffer Inuse        = 64K
```

```
IntfName: EZAISM01      IntfType: ISM       IntfStatus: Ready
  PFID: 0061  TRLE: IUT00061  PFIDStatues: Ready
  PNetID: PHYSICALNETWORK2
  GIDAddr:  8002000900090061
  Interface Statistics:
    BytesIn                          = 0
    Inbound Operations               = 0
    BytesOut                         = 0
    Outbound Operations              = 0
    SMC Links                        = 0
    TCP Connections                  = 0
    Intf Receive Buffer Inuse        = 0K
    Device Interrupts                = 0
```

```
IPv4 LAN Group Summary
 LanGroup: 001

   Name              Status      ArpOwner          VipaOwner
   -------           ------      --------          ---------
   TR1               Active      TR1               No

 LanGroup: 002

   Name              Status      ArpOwner          VipaOwner
   -------           ------      --------          ---------
   OSAQDIOLINK       Active      OSAQDIOLINK       Yes
   OSAQDIOINTF       Active      OSAQDIOINTF       No

IPv6 LAN Group Summary
 LanGroup: 004

   Name              Status      NDOwner           VipaOwner
   --------          ------      --------          ---------
   OSAQDIO46         Active      OSAQDIO46         Yes
```

```
NETSTAT DEVLINKS SMC
MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPIP1          12:04:57
IntfName: EZAISM01      IntfType: ISM       IntfStatus: Ready
  PFID: 0061  TRLE: IUT00061  PFIDStatues: Ready
  PNetID: PHYSICALNETWORK2
  GIDAddr:  8002000900090061
  Interface Statistics:
    BytesIn                          = 0
    Inbound Operations               = 0
    BytesOut                         = 0
    Outbound Operations              = 0
    SMC Links                        = 0
    TCP Connections                  = 0
    Intf Receive Buffer Inuse        = 0K
    Device Interrupts                = 0
  SMCD Link Information:
    LocalSMCLinkId: 00000000  RemoteSMCLinkId: 00000000
        VLANid: None
        LocalGID:  8003000900090061
        RemoteGID: 0000000000000000
        SMCLinkBytesIn:            0
        SMCLinkInOperations:       0
        SMCLinkBytesOut:           0
        SMCLinkOutOperations:      0
        TCP Connections:           0
        Link Receive Buffer Inuse: 0K

IntfName: EZARIUT10005      IntfType: RNIC       IntfStatus: Ready
  PFID: 0005  PortNum: 1  TRLE: IUT10005
  PNetID: NETWORK3
  VMACAddr: 02000012F030
  GIDAddr:  fe80::200:ff:fe12:f030
  Interface Statistics:
    BytesIn                          = 18994
    Inbound Operations               = 146
    BytesOut                         = 19139
    Outbound Operations              = 811
    SMC Links                        = 2
    TCP Connections                  = 1
    Intf Receive Buffer Inuse        = 64K
  SMCR Link Information:
    LocalSMCLinkId: FB710601  RemoteSMCLinkId: 72420601
      SMCLinkGroupId: FB710600  VLANid: 100  MTU: 1024
      LocalGID:  fe80::200:ff:fe12:f030
        LocalMACAddr:  02000012F030  LocalQP:  00004B
      RemoteGID: fe80::200:1ff:fe12:f030
        RemoteMACAddr: 02000112F030  RemoteQP: 00004A
      SMCLinkBytesIn:            498
      SMCLinkInOperations:       12
      SMCLinkBytesOut:           294
      SMCLinkOutOperations:      13
      TCP Connections:           0
      Link Receive Buffer Inuse: 0K
        64K   Buffer Inuse:      0K

  SMCR Link Information:
    LocalSMCLinkId: FB710701  RemoteSMCLinkId: 72420701
      SMCLinkGroupId: FB710700  VLANid: 100  MTU: 4096
      LocalGID:  fe80::200:ff:fe12:f030
        LocalMACAddr:  02000012F030  LocalQP:  00004C
      RemoteGID: fe80::200:1ff:fe12:f030
        RemoteMACAddr: 02000112F030  RemoteQP: 00004D
      SMCLinkBytesIn:            293
      SMCLinkInOperations:       8
      SMCLinkBytesOut:           490
      SMCLinkOutOperations:      15
      TCP Connections:           1
      Link Receive Buffer Inuse: 64K
        64K   Buffer Inuse:      64K
```

```
IntfName: EZARIUT10006      IntfType: RNIC       IntfStatus: Ready
  PFID: 0006  PortNum: 1  TRLE: IUT10006
  PNetID: NETWORK3
  VMACAddr: 02000012EF50
  GIDAddr:  fe80::200:ff:fe12:ef50
  Interface Statistics:
    BytesIn                          = 226
    Inbound Operations               = 4
    BytesOut                         = 29
    Outbound Operations              = 4
    SMC Links                        = 2
    TCP Connections                  = 1
    Intf Receive Buffer Inuse        = 64K

  SMCR Link Information:
    LocalSMCLinkId: FB710602  RemoteSMCLinkId: 72420602
      SMCLinkGroupId: FB710600  VLANid: 100  MTU: 2048
      LocalGID:  fe80::200:ff:fe12:ef50
        LocalMACAddr:  02000012EF50  LocalQP:  00004A
      RemoteGID: fe80::200:1ff:fe12:ef50
        RemoteMACAddr: 02000112EF50  RemoteQP: 00004B
      SMCLinkBytesIn:            226
      SMCLinkInOperations:       5
      SMCLinkBytesOut:           29
      SMCLinkOutOperations:      4
      TCP Connections:           1
      Link Receive Buffer Inuse: 64K
        64K   Buffer Inuse:      64K

  SMCR Link Information:
    LocalSMCLinkId: FB710702  RemoteSMCLinkId: 72420702
      SMCLinkGroupId: FB710700  VLANid: 100  MTU: 1024
      LocalGID:  fe80::200:ff:fe12:ef50
        LocalMACAddr:  02000012EF50  LocalQP:  00004D
      RemoteGID: fe80::200:1ff:fe12:ef50
        RemoteMACAddr: 02000112EF50  RemoteQP: 00004C
      SMCLinkBytesIn:            0
      SMCLinkInOperations:       0
      SMCLinkBytesOut:           0
      SMCLinkOutOperations:      0
      TCP Connections:           0
      Link Receive Buffer Inuse: 0K
        64K   Buffer Inuse:      0K
```

```
SMCR Link Group Information:
  SMCLinkGroupId: FB710600  PNetID: NETWORK3
    Redundancy: Full
    Link Group Receive Buffer Total: 3M
      64K   Buffer Total: 1M

    LocalSMCLinkId  RemoteSMCLinkId
    --------------  ---------------
    FB710601        72420601
    FB710602        72420602

  SMCLinkGroupId: FB710700  PNetID: NETWORK3
    Redundancy: Full
    Link Group Receive Buffer Total: 3M
      64K   Buffer Total: 1M

    LocalSMCLinkId  RemoteSMCLinkId
    --------------  ---------------
    FB710701        72420701
    FB710702        72420702
```

```
Netstat DEvlinks/-d PNETID *
MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS1          12:17:36
PNetID: PHYSICALNETWORK2
  IntfName: IQDIOLNK0A3D0001  IntfType: IPAQIDIO
  IntfName: IQDIOINTF6        IntfType: IPAQIDIO6
  IntfName: EZAISM01          IntfType: ISM        Associated: Yes
PNetID: NETID1
  IntfName: QDIO4SHRL         IntfType: IPAQENET
  IntfName: QDIO6SHR          IntfType: IPAQENET6
  IntfName: EZAISM02          IntfType: ISM        Associated: Yes
  IntfName: EZARIUT1A003      IntfType: RNIC       Associated: Yes
  IntfName: EZARIUT1A004      IntfType: RNIC       Associated: Yes
PNetID: PHYSICALNETWORK2
  IntfName: IQDIOLNK0A3D0001  IntfType: IPAQIDIO
  IntfName: IQDIOINTF6        IntfType: IPAQIDIO6
  IntfName: EZAISM01          IntfType: ISM        Associated: Yes
PNetID: NETID1
  IntfName: QDIO4SHRL         IntfType: IPAQENET
  IntfName: QDIO6SHR          IntfType: IPAQENET6
  IntfName: EZAISM02          IntfType: ISM        Associated: Yes
  IntfName: EZARIUT1A003      IntfType: RNIC       Associated: Yes
  IntfName: EZARIUT1A004      IntfType: RNIC       Associated: Yes
```

```
Netstat DEvlinks/-d PNETID PHYSICALNETWORK2
MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS1          12:31:45
IntfName: IQDIOLNK0A3D0001  IntfType: IPAQIDIO
  TRLE: IUTIQDIO  CHPID: FE  VChid: 0000
  Datapath: 0E02  SMCD: Yes

IntfName: IQDIOINTF6        IntfType: IPAQIDIO6
  TRLE: IUTIQDIO  CHPID: FE  VChid: 0000
  Datapath: 0E02  SMCD: Yes

IntfName: EZAISM01          IntfType: ISM        Associated: Yes
  TRLE: IUT00061  PFID: 0061  VChid: 7700
  GIDAddr: 8002000900090061
```

Example output for an OSAENTA interface:

```
OSA-Express Network Traffic Analyzer Information:
  OSA PortName: QDIO4101          OSA DevStatus:     Ready
    OSA IntfName: EZANTAQDIO4101  OSA IntfStatus:    Ready
    OSA Speed:    1000            OSA Authorization: Logical Partition
    OSAENTA Cumulative Trace Statistics:
      DataMegs:   0                   Frames:          8
      DataBytes:  760                 FramesDiscarded: 4
      FramesLost: 0
    OSAENTA Active Trace Statistics:
      DataMegs:   0                   Frames:          8
      DataBytes:  760                 FramesDiscarded: 4
      FramesLost: 0                   TimeActive:      8
    OSAENTA Trace Settings:          Status: On
      DataMegsLimit: 1024             FramesLimit:     2147483647
      Abbrev:        224              TimeLimit:       10080
      Discard:       ALL
    OSAENTA Trace Filters:           Nofilter: ALL
      DeviceID: *
      Mac:      *
      VLANid:   *
      ETHType:  *
      IPAddr:   *
      Protocol: *
      PortNum:  *
```

Report field descriptions

DevName
The device name that is configured on the DEVICE statement.

DevType
The device type that is configured on the DEVICE statement.

DevNum
The device number that is configured on the DEVICE statement. This field is significant only for device types CTC, CLAW, LCS, and CDLC.

DevStatus
The device status. You can use this field if you are having activation problems with the device or interface. Table 13 describes the possible status values:

Table 13. Possible device status values

Device status	Description
Starting	A START of the device has been issued by the operator, and TCP/IP has sent an Activation request to the Data Link Control (DLC) layer.
Sent SETUP	DLC has acknowledged the TCP/IP Activation request, and TCP/IP has requested DLC to perform the initial I/O sequence with the device.
Enabling	DLC has acknowledged the TCP/IP Activation request, and TCP/IP has requested DLC to allow data connections to be established for the device.
Connecting	DLC has accepted the Initial I/O Sequence request.
Connecting2	The control connection for a CLAW device has been established, and the second connection (on which IP traffic is carried) is being established.
Negotiating	The initial I/O sequence with the device is complete, and TCP/IP is performing additional link-layer initialization.
Ready	The initialization sequence with the device is complete. The device is now ready.
Deactivating	DLC has performed the first stage of an orderly device deactivation.
Not active	The device is not active. (The device has never been started, or has been stopped after having been started.)

Configured router status (CfgRouter)
The router attribute (PRIROUTER/SECROUTER/NONROUTER) that is specified on the DEVICE or INTERFACE statement. This field is significant only for MPCIPA devices and for IPAQENET and IPAQENET6 interfaces. This field is not displayed if virtual MAC (VMAC) has been configured.

Actual router status (ActRouter)
The router attribute in effect for the device or interface. It matches the configured router status unless the configured value conflicted with the configured value of another stack that is sharing the adapter. This field is significant only for MPCIPA devices and for IPAQENET and IPAQENET6 interfaces. The router attribute is determined when the device or interface starts. This field is not displayed if virtual MAC (VMAC) has been configured.

Virtual MAC address (VMACAddr)
The virtual local hardware address for this link or interface. This field is significant for the following types of devices:

- An IPAQENET link or interface, or an IPAQENET6 interface, where a virtual MAC address was configured by specifying the VMAC parameter. The value `n/a` is displayed if VMAC was configured but a virtual MAC address was not configured.
- An RNIC interface that is created when an IPAQENET or IPAQENET6 interface specified SMCR. The VMAC address is provided by VTAM, and is not configured on the INTERFACE profile statement. `VMACAddr` is displayed for active RNIC interfaces only.

Virtual MAC origin (VMACOrigin)
Displays whether the virtual MAC address (VMACAddr) was configured on the LINK or INTERFACE statement, or was generated by OSA-Express. This field is significant only for IPAQENET links or interfaces and for IPAQENET6 interfaces for which virtual MAC (VMAC) has been configured. The following list shows the possible values:

Cfg The virtual MAC address is configured on the LINK statement or on the INTERFACE statement.

OSA The virtual MAC address has been generated by OSA-Express.

Virtual MAC router status (VMACRouter)
Displays the virtual MAC router attribute that was specified on the LINK or INTERFACE statement using the ROUTEALL or ROUTELCL keywords. This field is significant only for IPAQENET links or interfaces and for IPAQENET6 interfaces for which virtual MAC (VMAC) has been configured. See OSA Routing information in the z/OS Communications Server: IP Configuration Guide for more information about Virtual MAC router attributes. The following list shows the possible values:

All Corresponds to the ROUTEALL keyword. Indicates that all IP traffic destined to the Virtual MAC is forwarded by the OSA-Express device to the TCP/IP stack

Local Corresponds to the ROUTELCL keyword. Indicates that only traffic destined to the Virtual MAC whose destination IP address is registered with the OSA-Express device by this TCP/IP stack is forwarded by the OSA-Express device.

Configured packing status (CfgPacking)
This field is the packing attribute (Packed/None) specified on the DEVICE statement. This field is significant only for CLAW devices.

Actual packing status (ActPacking)
This field indicates the packing attribute in effect for the device. It will match the configured packing status unless packing was requested and the device does not support packing. This field is significant only for a CLAW device and is determined when the device starts.

LnkName/IntfName
This field is the link name or the interface name of the particular device or interface being displayed. If the device or interface is configured, this field is the link name configured in the LINK statement or the interface name configured in the INTERFACE statement. If the link name or interface name is dynamically generated by the TCP/IP stack, this field is the dynamically generated link name or interface name.

LnkType/IntfType
This field is the link type or the interface type of the particular device or interface being displayed. If the device or interface is configured, this field is the link type configured in the LINK statement or the interface type configured in the INTERFACE statement. If the link type or interface type is dynamically generated by the TCP/IP stack, this field is the dynamically generated link type or interface type. .

LnkStatus/IntfStatus
This field is the link or interface status. The following list describes the possible link or interface status values:

Link/Interface status	Description
Ready	A START of the device/interface has been issued by the operator, and TCP/IP has been sent an Activation request to the Data Link Control (DLC) layer.
Not Active	The link or interface is not active. There is no command to start a link; link activation is normally performed during START device processing. Interface activation is performed during START interface processing. A link or interface is marked Not Active when: • The device or interface has not yet been started. • A failure has been encountered during the link or interface activation phase. (Such a failure produces an error message to the operator console, indicating the cause.)
DAD Pend	Duplicate Address Detection (DAD) for the link-local address is in progress on the IPv6 interface.

PortName
The name of the OSA-Express port. This is the value that was specified on the PORTNAME parameter on the INTERFACE statement. This field is significant only for IPAQENET and IPAQENET6 interfaces.

Datapath
The subchannel address that is associated with the TRLE definition. This value is one of the addresses that was specified on the DATAPATH parameter on the TRLE definition and is the subchannel address that VTAM assigned to this interface. If VTAM has not yet assigned a subchannel address to this interface, then this field contains the value `Unknown`. This field is significant only for IPAQENET, IPAQIDIO, IPAQENET6, and IPAQIDIO6 interfaces.

DatapathStatus
The datapath status. This field is significant only for IPAQENET, IPAQIDIO, IPAQENET6 , and IPAQIDIO6 interfaces. This field contains information that is useful if the interface is not activating correctly. See Table 13 on page 373 for possible status values.

CHPIDType
The CHPID type that is associated with this interface. This value was specified on the CHPIDTYPE parameter on the INTERFACE statement (or was generated by the stack) for OSA-Express QDIO interfaces. This field is significant only for IPAQENET and IPAQENET6 interfaces. The possible values and meanings are:

OSD A CHPID with connectivity to the external data network

OSX A CHPID with connectivity to the intra ensemble data network

OSM A CHPID with connectivity to the intra node management network

IPAddr
The IP address and optional number of bits (leftmost significant bits), which identifies the subnet mask of the interface. This value was specified on the IPADDR parameter on the INTERFACE statement. This field is significant for IPAQENET interfaces only. If the interface is defined with the TEMPIP keyword, the IP address is 0.0.0.0.

CHPID
The CHPID value that is associated with this interface. For HiperSockets, this value was specified on the CHPID parameter on the INTERFACE statement for predefined HiperSockets interfaces or is the value obtained from VTAM for HiperSockets interfaces that are created by dynamic XCF definitions. For OSA-Express QDIO interfaces that are configured with CHPIDTYPE OSX, this value was specified on the CHPID parameter. This field is significant only for IPAQIDIO, IPAQIDIO6, IPAQENET, or IPAQENET6 interfaces.

SMCR
Indicates whether this interface can be used for new TCP connections for Shared Memory Communications over Remote Direct Memory Access (SMC-R) for external data network communications. This value was specified on the SMCR or NOSMCR parameter on the INTERFACE statement for OSA-Express QDIO interfaces. This field is significant only for IPAQENET and IPAQENET6 interfaces. The possible values and meanings are:

YES Indicates that this interface can be used for new TCP connections to communicate with other stacks on the external data network by using SMC-R.

For an inactive interface, Yes means the interface is configured for SMC-R. An interface is configured for SMC-R when the SMCR parameter was specified on the INTERFACE statement or is in effect by default.

For an active interface, Yes means the interface is enabled for SMC-R. An interface is enabled for SMCR when the following conditions are true:

- The SMCR parameter was specified on the INTERFACE statement or is in effect by default.
- The TCP/IP stack is enabled for SMC-R. A TCP/IP stack is enabled for SMC-R when the SMCR parameter was specified on the GLOBALCONFIG statement.
- A physical network ID value was configured in HCD for this interface.

NO Indicates that this interface cannot be used for new TCP connections to communicate with other stacks on the external data network by using SMC-R. The NOSMCR parameter was specified on the INTERFACE statement.

Disabled (*reason_text***)**
Indicates that this interface was configured to communicate with other stacks on the external data network by using SMC-R, but SMC-R cannot be used for new TCP connections because of one of the following reasons:

No PNetID
No physical network ID value was configured in HCD for this interface. The physical network ID is learned during interface activation so this reason text is valid only for an active interface.

GLOBALCONFIG NOSMCR
The TCP/IP stack was not enabled for SMC-R.

No Subnet Mask
No subnet mask was configured on the INTERFACE statement for this interface.

SMCD
Indicates whether this interface can be used for new TCP connections for Shared Memory Communications - Direct Memory Access (SMC-D). This value was specified on the SMCD or NOSMCD parameter on the INTERFACE statement for OSA-Express QDIO or HiperSockets interfaces. This field is significant only for IPAQENET, IPAQIDIO, IPAQENET6, and IPAQIDIO6 interfaces. The possible values and meanings are:

YES Indicates that this interface can be used for new TCP connections to communicate with other stacks by using SMC-D.

For an inactive interface, Yes means the interface is configured for SMC-D. An interface is configured for SMC-D when the SMCD parameter was specified on the INTERFACE statement or is in effect by default.

For an active interface, Yes means the interface is enabled for SMC-D. An interface is enabled for SMC-D when the following conditions are true:

- The SMCD parameter was specified on the INTERFACE statement or is in effect by default.
- The TCP/IP stack is enabled for SMC-D. A TCP/IP stack is enabled for SMC-D when the SMCD parameter was specified on the GLOBALCONFIG statement.
- A physical network ID value was configured in HCD for this interface.

NO Indicates that this interface cannot be used for new TCP connections to communicate with other stacks by using SMC-D. The NOSMCD parameter was specified on the INTERFACE statement.

Disabled (*reason_text***)**
Indicates that this interface was configured to communicate with other stacks by using SMC-D, but SMC-D cannot be used for new TCP connections because of one of the following reasons:

No PNetID
No physical network ID value was configured in HCD for this interface. The physical network ID is learned during interface activation so this reason text is valid only for an active interface.

GLOBALCONFIG NOSMCD
The TCP/IP stack was not enabled for SMC-D.

No Subnet Mask
No subnet mask was configured on the INTERFACE statement for this interface.

PNetID MisConfig
The PNetID configured in HCD for this OSD interface matches the PNetID learned for a HiperSockets interface, or the PNetID configured in HCD for this HiperSockets interface matches the PNetID learned for an OSD interface. To use SMC-D, OSD interfaces must be configured on different PNetIDs from HiperSockets interfaces. The PNetID is learned during interface activation so this reason text is valid only for an active interface.

PFID The Peripheral Component Interconnect Express (PCIe) function ID (PFID) value that defines a 10GbE RoCE Express feature or an internal shared memory (ISM) device.

- For a RoCE Express feature, this value is specified on the SMCR PFID parameter of the GLOBALCONFIG TCP/IP profile statement. This field is significant only for RNIC interfaces that are created when an IPAQENET or IPAQENET6 interface specifies SMCR or takes SMCR as the default setting.
- For an ISM device, this value is learned dynamically during ISM device activation and is provided by VTAM to the TCP/IP stack. This field is significant only for ISM interfaces that are created when an IPAQENET, IPAQIDIO, IPAQENET6, or IPAQIDIO6 interface specifies SMCD or takes SMCD as the default setting.

PortNum
Specifies the 10GbE RoCE Express port number that is used for the associated PFID. The PortNum value is specified with the PFID value on the SMCR parameter of the GLOBALCONFIG statement in the TCP/IP profile.

PNetID
The physical network ID value that is configured in HCD for an interface. This field is significant only for IPAQIDIO or IPAQENET interfaces defined by using the INTERFACE statement, IPAQIDIO6 interfaces, IPAQENET6 interfaces, and active RNIC and ISM interfaces.

Interface	Value
Active OSD interfaces	• If a physical network ID is configured in HCD for the OSD interface, the configured value is displayed. • If no physical network ID is configured in HCD for the OSD interface, the value*None* is displayed. If the OSD interface is configured to use SMCR, a value of Disabled (No PNetID) is displayed in the SMCR field. If the OSD interface is configured to use SMCD, a value of Disabled (No PNetID) is displayed in the SMCD field.
Active OSX interfaces	The reserved value IEDN is used.

Interface	Value
Active HiperSockets interfaces	• If a physical network ID is configured in HCD for the HiperSockets interface, the configured value is displayed. • If no physical network ID is configured in HCD for the HiperSockets interface, the value*None* is displayed. If the HiperSockets interface is configured to use SMCD, a value of Disabled (No PNetID) is displayed in the SMCD field.
Active ISM interfaces	The value that is configured in HCD for the ISM interface is displayed. If no value is configured in HCD, activation of the ISM interface fails.
Active RNIC interfaces	The value that is configured in HCD for the RNIC interface is displayed. If no value is configured in HCD, activation of the RNIC interface fails.

TRLE The name of the TRLE that is associated with this interface. This field is significant only for MPCPTP6, IPAQIDIO, IPAQIDIO6, ISM and RNIC interfaces.

For MPCPTP6 interfaces
This value was specified on the TRLE parameter of the INTERFACE statement for predefined MPC interfaces or is the value obtained from VTAM for MPC interfaces that are created by dynamic XCF definitions.

For IPAQIDIO or IPAQIDIO6 interfaces
This value is obtained from VTAM for IPAQIDIO or IPAQIDIO6 interfaces that INTERFACE definitions create. This value is displayed for active interfaces only.

For ISM interfaces
This value is obtained from VTAM for ISM interfaces that are created dynamically during activation of IPAQENET, IPAQIDIO, IPAQENET6, or IPAQIDIO6 interfaces that specify SMCD or take SMCD as the default setting when SMC-D is enabled. This value is displayed only when the PFIDStatus value of the interface is Starting or Ready.

For RNIC interfaces
This value is obtained from VTAM for RNIC interfaces that are created for PFIDs configured on the GLOBALCONFIG statement when SMC-R is enabled. This value is displayed only when the PFIDStatus value of the interface is Starting or Ready.

PFIDStatus
This field is the RNIC or ISM interface PFID status. The following list describes several status values:

PFID status	Description
Ready	The initialization sequence with the PFID is complete. The PFID is ready.

PFID status	Description
Not Active	The PFID is not active. The PFID has never been started, or has been stopped after having been started.
Starting	A START command of the PFID has been issued, and TCP/IP has sent an Activation request to the Data Link Control (DLC) layer.
Deactivating	DLC has performed the first stage of an orderly PFID deactivation.

GidAddr
The group identifier (GID) value that is associated with the RNIC or ISM interface.

- When SMC-R is enabled, this value is obtained from VTAM for RNIC interfaces that are created for PFIDs configured on the GLOBALCONFIG statement when SMC-R is enabled. This value is displayed for active RNIC interfaces only.
- When SMC-D is enabled, this value is obtained from VTAM for ISM interfaces that are created for SMC-D processing. This value is displayed for active ISM interfaces only.

NetNum
The adapter number that was specified on the LINK statement. This field is significant only for CTC and LCS links.

QueSize
The queue size represents the number of outbound packets for this link or interface that are queued and waiting for ARP or neighbor resolution. This field is significant only for links on ATM and LCS devices and for IPAQENET6 interfaces.

Speed Indicates the interface speed (in million bits per second) that is reported by the device. This field is significant only for IPAQENET links or interfaces, ATM and IPAQTR links, and IPAQENET6 interfaces, and only if the link or interface is active.

MAC address order (MacAddrOrder)
Indicates the canonical option (CANON/NONCANON) that is specified on the LINK statement. This field is significant only for token-ring links.

SrBridgingCapability
Indicates whether the link supports source route bridging. This field is significant only for token-ring links.

IpBroadcastCapability
Indicates whether the link is broadcast capable. This field is significant only for links on LCS and MPCIPA devices and IPAQENET interfaces.

ArpBroadcastType
Indicates the ARP broadcast option (ALLRINGSBCAST/LOCALBCAST) that is specified on the LINK statement. This field is significant only for token-ring links.

ArpOffload
Indicates whether ARP processing is being offloaded to the adapter. This field is significant only for active links that support ARP offload.

ArpOffloadInfo
Indicates whether the adapter reports ARP offload data to TCP/IP. If so, then the ARP cache data can be displayed with the Netstat ARP/**-R** report even though the ARP function is being offloaded. This field is significant only for active links that support ARP offload.

Routing Parameters
This section displays routing information for IPv4 links that are defined with the DEVICE and LINK profile statements.

MTU Size
This value is determined in one of the following ways:

- If you are using OMPROUTE and the link is defined to OMPROUTE, the value might have been specified on the MTU parameter on the OSPF_INTERFACE, RIP_INTERFACE, or INTERFACE statement for the link. If one of these OMPROUTE statements was specified for the link but the MTU parameter was not specified, OMPROUTE sets the **MTU Size** value to 576.
- If you are using OMPROUTE, the link is not defined to OMPROUTE, and OMPROUTE is not configured to ignore undefined links, OMPROUTE sets the **MTU Size** value to 576.
- If you are not using OMPROUTE (or if the link is not defined to OMPROUTE), OMPROUTE is configured to ignore undefined links, and a BSDROUTINGPARMS profile statement was specified for the link, then the **MTU Size** value is configured using the BSDROUTINGPARMS profile statement MTU parameter.
- If none of the previously described methods provides an MTU Size value or if the MTU Size parameter does not apply to this link, then the value `n/a` is displayed.

To determine the MTU Size value that is being used by the stack for a link, see the ActMtu field for the link. To determine the MTU Size value that is being used for a route over this link, see the MTU field on the Netstat ROUTe/**-r** report.

Metric The routing metric that is associated with the link. This value is determined in one of the following ways:

- If you use OMPROUTE and the link is defined to OMPROUTE using the OSPF_INTERFACE statement, then the Metric value is configured using the Cost0 parameter on the OSPF_INTERFACE statement. If the Cost0 parameter is not specified, then OMPROUTE sets the value to 1.
- If you use OMPROUTE and the link is defined to OMPROUTE using the RIP_INTERFACE statement, then the Metric value is configured using the In_Metric parameter on the RIP_INTERFACE statement. If the In_Metric parameter is not specified, then OMPROUTE sets the value to 1.
- If you use OMPROUTE and the link is defined to OMPROUTE using the INTERFACE statement or if the link is not defined to OMPROUTE and OMPROUTE is not configured to ignore undefined links, then OMPROUTE sets the Metric value to 0.
- If you are not using OMPROUTE (or if the link is not defined to OMPROUTE) and OMPROUTE is configured to ignore undefined links, the Metric value is configured in one of the following ways:

- For dynamic XCF links, the Metric value is configured using the cost_metric value of the DYNAMICXCF parameter on the IPCONFIG profile statement.
- If a BSDROUTINGPARMS profile statement was specified for the link, the Metric value is configured using the cost_metric parameter of BSDROUTINGPARMS profile statement.

- If none of the previously described methods provided a Metric value, the stack sets the value to 0

DestAddr

The destination address applies to point-to-point links only and is the IP Address of the other side of the point-to-point link. This value is determined in one of the following ways:

- If you are using OMPROUTE and the link is defined to OMPROUTE, then the value is configured using the Destination_Addr parameter on the OSPF_INTERFACE, RIP_INTERFACE, or INTERFACE statement. If the Destination_Addr parameter is not specified, then OMPROUTE sets the value to 0.
- If you are using OMPROUTE but the link is not defined to OMPROUTE and OMPROUTE is not configured to ignore undefined links, then OMPROUTE sets the value to 0.
- If you are not using OMPROUTE (or if the link is not defined to OMPROUTE), OMPROUTE is configured to ignore undefined links, and a BSDROUTINGPARMS profile statement was specified for the link, then the value is configured using the dest_addr parameter for this statement.
- If none of these methods has provided a destination address value, then the stack sets a default value in one of the following ways:
  - For links other than point-to-point links, the value is set to 0.
  - For point-to-point links, the value is set as follows:
    - If routes are defined over the link, then the stack sets the value using the gateway address of an indirect route or the destination address of a direct host route.
    - If no routes are defined over the link, then the value is set to 0.

SubnetMask

The subnet mask that is associated with the link. This value is determined in one of the following ways:

- If you are using OMPROUTE and the link is defined to OMPROUTE, then the value is configured using the Subnet_Mask parameter on the OSPF_INTERFACE, RIP_INTERFACE, or INTERFACE statement.
- If you are using OMPROUTE, the link is not defined to OMPROUTE, and OMPROUTE is not configured to ignore undefined links, then OMPROUTE assigns a value based on the IP address that is assigned to the link.
- If you are not using OMPROUTE (or if the link is not defined to OMPROUTE) and OMPROUTE is configured to ignore undefined links, then the value is assigned in one of the following ways:

- For dynamic XCF links, the value is configured using the *subnet_mask* or *num_mask_bits* value of the DYNAMICXCF parameter on the IPCONFIG profile statement.
- For dynamic VIPA links, the value is configured using the *address_mask* parameter on the VIPADEFINE, VIPABACKUP, or the VIPARANGE profile statement.
- If a BSDROUTINGPARMS profile statement was specified for the link, the value is configured using the *subnet_mask* parameter for the BSDROUTINGPARMS profile statement.

• If none of the previously described methods provides a subnet mask value, then the stack assigns a value based on the IP address that is assigned to the link.

Packet trace settings

Use the PKTTRACE statement to control the packet tracing facility in TCP/IP. You can use this statement to select IP packets as candidates for tracing and subsequent analysis. An IP packet must meet all of the conditions specified on the statement for it to be traced.

Protocol
The protocol number from the PROT keyword of the PKTTRACE command or * if not specified.

TrRecCnt
The number of packets traced for this PKTTRACE command.

PckLength
The value of the ABBREV keyword of the PKTTRACE command or FULL to capture the entire packet.

SrcPort
The port number from the SRCPORT parameter of the PKTTRACE command or profile statement. If an asterisk (*) is displayed, then either a port number was not specified for the SRCPORT parameter, or the PORTNUM parameter was also specified. If both the SrcPort and PortNum fields contain a value *, then the IP packets are not being filtered by the source port.

DestPort
The port number from the DESTPORT parameter of the PKTTRACE command or profile statement. If an asterisk (*) is displayed, then either a port number was not specified for the DESTPORT parameter, or the PORTNUM parameter was also specified. If both the DestPort and PortNum fields contain an asterisk (*), then the IP packets are not being filtered by destination port.

PortNum
The port number from the PORTNUM parameter of the PKTTRACE command or profile statement. If an asterisk (*) is displayed, then either a port number was not specified for the PORTNUM parameter, or the DESTPORT or SRCPORT parameters were also specified. If the PortNum, SrcPort, and DestPort fields all contain an asterisk (*), then the IP packets are not being filtered by port.

Discard
The value specified for the PKTTRACE DISCARD parameter. A numerical value is a discard reason code. The value NONE, which

is the default, indicates that only packets that were delivered are being traced. The value ALL indicates that only discarded IP packets are being traced. The value asterisk (*) indicates that discarded IP packets and delivered IP packets are being traced.

IpAddr
The IP address from the IPADDR keyword of the PKTTRACE command or asterisk (*) if not specified.

SubNet
The IP subnet mask from the SUBNET keyword of the PKTTRACE command or asterisk (*) if not specified.

ATM Specific
This section contains information about ATM links:

ATM PortName
The PORTNAME value specified on the DEVICE statement.

For an ATM link configured as a Permanent Virtual Circuit (PVC), the following additional fields are displayed:

ATM PVC Name
The name of the PVC specified on the ATMPVC statement.

PVC Status
This field can have the following values:

ATM PVC status	Description
Not Active	The PVC is not active. There is no command to start a PVC; PVC activation is normally attempted during START device processing. A PVC is marked Not Active when: • The device has not yet been started. • The remote side of the PVC is not active. • A failure has been encountered during the PVC activation phase. (Such a failure produces an error message to the operator.)
Ready	The initialization sequence for the PVC is complete. The PVC is now ready for use.

For an ATM link configured as a Switched Virtual Circuit (SVC), the following additional fields are displayed:

ATM LIS Name
The name of the ATM Logical IP Subnet (LIS) specified on the ATMLIS statement.

SubnetValue
The subnet_value specified on the ATMLIS statement.

SubnetMask
The subnet_mask specified on the ATMLIS statement.

DefaultMTU
The DFLTMTU value specified on the ATMLIS statement.

InactvTimeOut
The INACTVTO value specified on the ATMLIS statement.

MinHoldTime
The MINHOLD value specified on the ATMLIS statement.

MaxCalls
The maximum number of SVCs that can be active for this ATMLIS.

CachEntryAge
The CEAGE value specified on the ATMLIS statement.

ATMArpReTry
The ARPRETRIES value specified on the ATMLIS statement.

ATMArpTimeOut
The ARPTO value specified on the ATMLIS statement.

PeakCellRate
The PEAKCR value specified on the ATMLIS statement.

NumOfSVCs
The number of currently active SVCs for this ATMLIS.

BearerClass
The BEARERCLASS value specified on the ATMLIS statement.

For an ATM SVC link that is configured with an ATM ARP server, the following additional fields are displayed:

ATMARPSV Name
The name of the ATM ARP server specified on the ATMARPSV statement.

VcType
Indicates whether the ATM ARP server connection is a PVC or an SVC. This value comes from the ATMARPSV statement.

ATMaddrType
The ATM address type specified on the ATMARPSV statement. The only supported value is NSAP.

ATMaddr
The ATM address of the ATM ARP server. If the connection to the ATM ARP server is an SVC, then this is the physical_addr value specified on the ATMARPSV statement. For a PVC connection to the ATM ARP server, this is the remote ATM address learned by TCP/IP when the PVC was activated.

IpAddr
The IP address of the ATM ARP server. If the connection to the ATM ARP server is an SVC, then this is the ip_addr value specified on the ATMARPSV statement. For a PVC connection to the ATM ARP server, this is the remote IP address learned by TCP/IP when the PVC was activated.

Multicast Specific
This section displays multicast information for the link or interface.

Multicast Capability
Indicates whether the link or interface is multicast capable.

- For point-to-point interfaces, the value of this field is always `Yes`.
- For LCS and MPCIPA links and IPAQENET, IPAQENET6, IPAQIDIO, and IPAQIDIO6 interfaces, the multicast capability is known only after the link or interface is active. If the link or interface is not active, the multicast capability value is `Unknown`.

- For IPAQIQDX6 interfaces, the value of this field is always `ND only`, the interface is multicast capable but multicast processing is used only for neighbor discovery.

If the link or interface is multicast capable then the following additional fields are displayed for each multicast group for which the link or interface is receiving data. There is no limit to the number of multicast groups for which a link or interface can receive data. For IPAQIQDX6 interfaces, the multicast groups indicate only neighbor discovery processing.

Group The multicast group address for which this link or interface is receiving data.

RefCnt
The number of applications that are receiving data for this multicast group.

SrcFltMd
The source filter mode indicates the type of multicast source IP address filtering that has been configured at the interface. Source IP address filtering can be done by either an IGMPv3 or MLDv2-capable multicast router on a per interface basis or by the host on a per socket basis. The host provides its source filter mode and source IP address filter list for each multicast group that an application has joined on the interface with any IGMPv3 and MLDv2-capable multicast routers that are connected to the interface. This permits IGMPv3-capable and MLDv2-capable multicast routers to send only multicast packets that have been requested by at least one host on the subnet to which the interface is connected. If the multicast packets are not filtered by an IGMPv3-capable or MLDv2-capable multicast router (for example the router does not support IGMPv3 or MLDv2), or if there are multiple hosts on the local area network that have either a different source filter mode or a different source IP address filter list for a given multicast group, the host uses the source IP address filter information to ensure that each application receives only packets that it has requested.

The value is either Include or Exclude. A source filter applies only to incoming multicast data. The source filter applies to all the IP addresses in the SrcAddr fields for the associated multicast group address and the link or the interface. The source filter mode and the corresponding source filter IP addresses are configured by applications for their UDP or RAW sockets that have joined the multicast group for this interface. See the information about Designing multicast programs in the z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference for details about how applications configure these values for a socket.

Include
Indicates that the interface or link receives only multicast datagrams that have a source IP address that matches an IP address indicated in the SrcAddr field.

Exclude
Indicates either that the source filter function is not active or that the interface or link receives only multicast

datagrams that have a source IP address that does not match an IP address indicated in the SrcAddr field. If the source filter function is not active or if the source filter function is active but no SrcAddr value is set, the SrcAddr field contains the value None.

SrcAddr
Source address information for the socket.

ipaddr The source IP address that is used in conjunction with the SrcFltMd value to determine which incoming multicast datagrams are received by the interface.

None This value is displayed only when the source filter function is not configured for the interface or when the source filter mode is Exclude but there was no intersection of excluded source IP addresses among the sockets for the same multicast group address and interface.

Source VIPA interface (SrcVipaIntf)
The name of the VIPA that is used for this interface if source VIPA is in effect. This is the value that was specified on the SOURCEVIPAINTERFACE parameter on the INTERFACE statement. This field is significant only for IPAQENET, IPAQENET6, IPAQIDIO6, and MPCPTP6 interfaces.

Duplicate address detection (DupAddrDet)
The DUPADDRDET value specified on the INTERFACE statement. This field is significant only for IPAQENET6 interfaces.

Interface ID (IntfID)
The INTFID value specified on the INTERFACE statement. This field is significant only for IPAQENET6, IPAQIDIO6, and MPCPTP6 interfaces.

MAC address (MacAddress)
The local hardware address for this link or interface. This field is significant only for links on LCS devices and for IPAQENET6 interfaces. This field is displayed only if the link or interface is active and if virtual MAC (VMAC) is not configured.

Router Hop Limit (RtrHopLimit)
The value that is placed in the Hop Count field of the IP header for outgoing IP packets. This value was obtained from a received router advertisement and is significant only for IPAQENET6 interfaces. This field is displayed only when a nonzero hop limit value was received in a router advertisement over this interface and IGNOREROUTERHOPLIMIT is not configured on the IPCONFIG6 profile statement.

CfgMtu
The MTU value that was configured on the INTERFACE statement (or `None` if an MTU value was not configured). This field is significant only for IPAQENET, IPAQENET6, or IPAQIDIO interfaces.

ActMtu
The largest MTU that is supported by an active link or interface. If the link or interface is inactive, then this field displays Unknown. This field is significant for all links and interfaces except virtual ones.

VLANid
This field is significant only for IPAQENET links or interfaces, IPAQIDIO links, or IPAQENET6 and IPAQIDIO6 interfaces. This field indicates

whether a virtual LAN ID was configured on the VLANID parameter on the LINK or INTERFACE profile statement. The following values can be displayed in this field:

None
This value indicates that the VLANID parameter was not specified on the LINK or INTERFACE profile statement for the interface. For an IPAQIDIO link or IPAQIDIO6 interface that is dynamically generated as part of dynamic XCF HiperSockets processing, this value indicates that the IQDVLANID parameter was not specified on the GLOBALCONFIG profile statement.

n/a
This value indicates that the VLANID parameter was specified on the LINK or INTERFACE profile statement, but the interface does not support VLAN IDs.

vlanid
If an OSA-Express device is active and supports virtual LAN IDs, this field indicates that all IP packets through this OSA-Express link or interface from this stack are being tagged with this VLAN ID. For an active HiperSockets link or interface that supports virtual LAN IDs, this field indicates that all IP packets through this HiperSockets link or interface from this stack are associated with this VLAN ID.

VLANpriority
This field is significant only for active IPAQENET links or interfaces or IPAQENET6 interfaces. This field indicates whether all IP packets through this OSA-Express link or interface from this stack are being tagged with a VLAN priority. The possible values are:

Enabled
Indicates that all IP packets through this OSA-Express link or interface are being tagged with a VLAN priority. See z/OS Communications Server: IP Configuration Reference for information about the SetSubnetPrioTosMask statement and details about how to configure VLAN priorities.

Disabled
Indicates that the OSA-Express link or interface supports VLAN priority, but currently no VLAN priority values are defined. If the VLANid field displays `None` or `n/a`, all IP packets through this OSA-Express link or interface are not VLAN tagged. All other values indicate that all IP packets are VLAN tagged, but only with VLAN IDs, not with VLAN priority.

Unknown
Indicates that the VLAN priority tagging support for the OSA-Express is unknown because the link or interface is not yet active.

DynVLANRegCfg
This field is significant only for IPAQENET links or interfaces and IPAQENET6 interfaces. This field is displayed only under the following conditions:

- The link or interface is not yet active and a VLAN ID was specified.
- The link or interface is active, a VLAN ID value was specified, and the OSA-Express feature has accepted the VLAN ID value.

This field indicates whether dynamic VLAN ID registration was configured on the LINK or INTERFACE statement. The possible values are:

Yes
Indicates that the DYNVLANREG parameter was specified on the LINK or INTERFACE statement.

No Indicates that the NODYNVLANREG parameter was specified on the LINK or INTERFACE statement or is in effect by default.

DynVLANRegCap

This field indicates whether the OSA-Express feature that is represented by the LINK or INTERFACE statement is capable of supporting dynamic VLAN ID registration.This field is significant only for IPAQENET links or interfaces and IPAQENET6 interfaces. This field is displayed only under the following conditions:

- The link or interface is not yet active and a VLAN ID was specified.
- The link or interface is active, a VLAN ID value was specified, and the OSA-Express feature has accepted the VLAN ID value.

The possible values are:

Yes
Indicates that the OSA-Express feature is capable of supporting dynamic VLAN ID registration.

No Indicates that the OSA-Express feature is not capable of supporting dynamic VLAN ID registration.

Unknown
Indicates that the dynamic VLAN ID registration capability of the OSA-Express feature is unknown because the link or interface is not yet active.

ChecksumOffload
This field is significant only for active IPAQENET and IPAQENET6 links or interfaces. This field indicates whether the checksum offload support is in effect and is displayed only when the link or interface is active. The possible values are:

Yes Indicates that the checksum offload function is enabled on the adapter for this interface.

No Indicates that the checksum offload function is not enabled on the adapter for this interface.

Unsupported
Indicates that the checksum offload function is not supported on the adapter for this interface.

SegmentationOffload
This field is significant only for active IPAQENET and IPAQENET6 links or interfaces. This field indicates whether the TCP segmentation offload support is in effect and is displayed only when the link or interface is active. Possible values are:

Yes Indicates that the segmentation offload function is enabled on the adapter for this interface.

No Indicates that the segmentation offload function is not enabled on the adapter for this interface.

Unsupported
Indicates that the segmentation offload function is not supported on the adapter for this interface.

SecClass
This field identifies the security class value for IP filtering. This field applies to all IPv4 and IPv6 interfaces except virtual and loopback, but the value is in effect only if the IPSec function is active for the applicable IP version. You can use the Netstat CONFIG/**-f** command to determine whether IPSec is active. Valid security class values are in the range 1 - 255. The displayed value was defined by one of the following methods:

- By the SECCLASS parameter on the LINK or INTERFACE profile statement
- For dynamic XCF interfaces, by the DYNAMICXCF SECCLASS subparameter on the IPCONFIG or IPCONFIG6 profile statement
- For OSM interfaces, by the TCP/IP stack's automatic configuration of the interface, or by the IPSECURITY OSMSECCLASS subparameter on the IPCONFIG6 profile statement

MonSysplex
Indicates whether the status of this link or interface is being monitored by Sysplex Autonomics. This field is significant for all IPv4 links or interfaces except virtual, loopback, and all dynamically configured links, and for all IPv6 interfaces except virtual, loopback, and all dynamically configured interfaces.

Yes Indicates that the status of this link or interface is being monitored by Sysplex Autonomics. It is configured by specifying the MONSYSPLEX keyword on the LINK or INTERFACE profile statement and specifying the MONINTERFACE keyword for the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement. If DYNROUTE keyword is also coded on the GLOBALCONFIG SYSPLEXMONITOR profile statement, then the presence of dynamic routes over this link or interface is also monitored.

Configured
Indicates that this link or interface was configured to be monitored by Sysplex Autonomics. It was configured by specifying the MONSYSPLEX keyword on the LINK or INTERFACE profile statement, but the link or interface is not currently being monitored because the MONINTERFACE keyword was not specified on the SYSPLEXMONITOR parameter on the GLOBALCONFIG profile statement.

No Indicates that the status of this link or interface is not being monitored by Sysplex Autonomics because the MONSYSPLEX keyword was not specified on the LINK or INTERFACE profile statement.

Isolate
This field is significant only for IPAQENET interfaces (defined using the INTERFACE statement) and for IPAQENET6 interfaces. This field ndicates whether the OSA-Express device is prevented from routing packets directly to another stack that is sharing the OSA-Express connection. For more details, see OSA-Express connection isolation information in z/OS Communications Server: IP Configuration Guide.

No Indicates that this interface is eligible for OSA-Express direct

routing. Therefore, the OSA-Express device can route packets directly to another stack that is sharing the OSA-Express connection (as long as the interface from the other stack is also eligible for direct routing).

Yes Indicates that this interface is not eligible for OSA-Express direct routing. Therefore, the OSA-Express device cannot routing packets directly to another stack that is sharing the OSA-Express connection.

OptLatencyMode
This field is significant only for IPAQENET interfaces (defined using the INTERFACE statement) and for IPAQENET6 interfaces. The field indicates whether optimized latency mode (OLM) was configured for this OSA-Express interface. For more information about optimized latency mode, see optimized latency mode information in z/OS Communications Server: IP Configuration Guide. Possible values are:

No Indicates that the OSA-Express interface is not configured with optimized latency mode.

Yes
Indicates that the OSA-Express interface is configured with optimized latency mode. Optimized latency mode optimizes interrupt processing for both inbound and outbound data.

Disabled
Indicates that the OSA-Express interface was configured with optimized latency mode, but the function could not be enabled when the interface was activated. The most likely reason is that the OSA-Express interface does not support this function.

IQDMultiWrite
This field is significant only for active HiperSockets devices or interfaces. This field indicates whether the HiperSockets multiple write facility is currently being used for the device or interface. To configure the stack to use the HiperSockets multiple write facility, specify the IQDMULTIWRITE parameter on the GLOBALCONFIG profile statement. The possible values are:

Enabled
Indicates that the HiperSockets multiple write facility is currently being used for the device or interface.

Enabled (ZIIP)
Indicates that the HiperSockets multiple write facility is currently being used for the device or interface. Additionally, CPU cycles that are associated with the HiperSockets multiple write facility are to be displaced to an available zIIP.

Disabled
Indicates that the HiperSockets multiple write facility is not currently being used for the device or interface.

Unsupported
Indicates that theIBM z Systems environment does not support the HiperSockets multiple write facility.

ReadStorage
This field is significant only for active IPAQENET and IPAQIDIO links or

interfaces, IPAQTR links, and for IPAQIDIO6 and IPAQENET6 interfaces. This field indicates the amount of storage (in kilobytes) that is being used for read processing.

InbPerf
This field is significant only for IPAQENET links or interfaces, IPAQTR links, and IPAQENET6 interfaces. This field indicates how frequently the adapter interrupts the host. This field indicates how the processing of inbound traffic is performed. If the interface is not active, then this field shows the configured value. If the interface is active, then this field shows the value that is in effect. The possible values are:

Balanced
Indicates that the adapter is to use a static interrupt-timing value that strikes a balance between MinCPU and MinLatency.

Dynamic
This setting is significant only for IPAQENET links, and IPAQENET and IPAQENET6 interfaces. It indicates that the stack and the adapter are to dynamically update the frequency with which the adapter interrupts the host for inbound traffic.

WorkloadQueueing
This field is displayed only for IPAQENET and IPAQENET6 interfaces. It indicates whether QDIO inbound workload queueing is enabled. Possible values are:

Yes QDIO inbound workload queueing is in effect. The QDIO interface is defined using the INTERFACE statement with INBPERF DYNAMIC WORKLOADQ specified.

No QDIO inbound workload queueing is not in effect. The QDIO interface is defined using the INTERFACE statement with INBPERF DYNAMIC or INBPERF DYNAMIC NOWORKLOADQ specified.

Unsupported
QDIO inbound workload queueing was requested on the INTERFACE statement but the OSA-Express interface does not support it. QDIO inbound workload queueing is supported on OSA-Express3 or later features on an IBM System z10 GA3 or later CPC.

MinCPU
Indicates that the adapter is to use a static interrupt-timing value that minimizes host interrupts, and therefore minimizes host CPU consumption.

MinLatency
Indicates that the adapter is to use a static interrupt-timing value that minimizes latency delay by more aggressively presenting received packets to the host.

TempPrefix
This field is significant only for IPAQENET6 interfaces with stateless address autoconfiguration enabled. One or more TempPrefix fields are displayed. Together the TempPrefix fields indicate the set of prefixes for which temporary IPv6 addresses can be generated, if temporary addresses

are enabled on the IPCONFIG6 statement. The set of prefixes is specified on the TEMPPREFIX parameter on the INTERFACE statement. The possible values displayed are:

All IPv6 temporary addresses are generated for all prefixes that are learned from a router advertisement over this interface. This is the default.

Disabled
Autoconfiguration of temporary addresses for the interface is disabled because duplicate addresses were detected. Temporary addresses are not generated for this interface.

None Temporary addresses are not generated for this interface.

IPv6 prefix/prefix length
IPv6 temporary addresses are generated for all prefixes that are learned from a router advertisement over this interface and that are included in one of the prefixes in this prefix list.

Link/Interface Statistics
This section is significant for all links and interfaces except virtual ones. The following statistical information is displayed:

BytesIn
Number of bytes received over an interface.

Inbound Packets
The number of unicast inbound packets received over an interface. This value applies to all links and interfaces except for RNIC and ISMinterfaces.

Inbound Packets In Error
Number of inbound packets discarded because of an error validating the packet. This value applies to all links and interfaces except for RNIC and ISMinterfaces.

Inbound Packets Discarded
Number of inbound packets discarded because of an out-of-storage condition. This value applies to all links and interfaces except for RNIC and ISMinterfaces.

Inbound Packets With No Protocol
Number of inbound packets discarded because of an unknown protocol type. This value applies to all links and interfaces except for RNIC and ISMinterfaces.

BytesOut
Number of bytes transmitted over an interface.

Outbound Packets
The number of unicast outbound packets transmitted over an interface. This value applies to all links and interfaces except for RNIC and ISMinterfaces.

Outbound Packets In Error
Number of outbound packets discarded because of errors other than an out-of-storage condition. This value applies to all links and interfaces except for RNIC and ISM interfaces.

Outbound Packets Discarded
Number of outbound packets discarded because of an

out-of-storage condition. This value applies to all links and interfaces except for RNIC and ISMinterfaces.

Inbound Operations

- For RNIC interfaces, this is the number of Remote Direct Memory Access (RDMA) inbound operations processed across this interface.
- For ISM interfaces, this is the number of Internal Shared Memory inbound operations processed across this interface.

Outbound Operations

- For RNIC interfaces, this is the number of RDMA outbound operations processed across this interface.
- For ISM interfaces, this is the number of Internal Shared Memory outbound operations processed across this interface.

SMC Links

- For RNIC interfaces, this is the current number of SMC-R links between this stack and other stacks across this interface.
- For ISM interfaces, this is the current number of SMC-D links between this stack and other stacks across this interface.

TCP Connections

- For RNIC interfaces, this is the number of TCP connections across all the SMC-R links that are associated with this interface. One or more TCP connections can use the same SMC-R link.
- For ISM interfaces, this is the current number of TCP connections across all the SMC-D links that are associated with this interface. One or more TCP connections can use the same SMC-D link.

Intf Receive Buffer Inuse

- For RNIC interfaces, this is the amount of RMB storage in use by the TCP connections that are using SMC-R links associated with this interface.
- For ISM interfaces, this is the amount of DMB storage in use by the TCP connections that are using SMC-D links associated with this interface.

Device Interrupts

The number of real program controlled interrupts (PCI's) that the VTAM device interrupt exit fields for the ISM device. A real PCI is a dispatch of the device interrupt exit as a result of a call from the system interrupt handler.

Rule: This value is reset to 0 each time when the interface is deactivated.

IPv4 LAN Group Summary

The IPv4 LAN group summary lists links or interfaces that are takeover candidates for each other. The stack creates a LAN group when it detects redundant connectivity to a LAN. For each link or interface in the LAN group, this summary displays which link or interface owns ARP responsibility for that link or interface. The summary also displays which link or interface owns the ARP responsibility in the LAN group for any VIPAs.

IPv6 LAN Group Summary

The IPv6 LAN group summary lists interfaces that are takeover candidates for each other. The stack creates a LAN group when it detects redundant connectivity to a LAN. For each interface in the LAN group, this summary displays which interface owns neighbor discovery (ND) address resolution responsibility for that interface. The summary also displays which interface owns the ND Address Resolution responsibility in the LAN group for any VIPAs.

LanGroup
Identifies the LAN group. This identifier is assigned by the stack and represents a group of interfaces on the same LAN. This identifier is not a VLAN ID.

Name The link name configured on the LINK statement or the interface name configured on the INTERFACE statement.

Status The link or interface status. Valid values are Active or Not Active.

ArpOwner
The link or interface name that owns ARP responsibility for this link or interface in the LAN group. An active link or interface owns its ARP responsibility.

NDOwner
The interface name that owns neighbor discovery (ND) responsibility for this interface in the LAN group. An active interface owns its ND responsibility.

VipaOwner
Indicates whether the link or interface owns the ARP or ND responsibility for the VIPAs in the LAN group.

Associated IQDX Interface

The name of the Internal Queued Direct I/O extensions function (IQDX) interface that is associated with this OSX interface. This section is significant for OSX interfaces that use an IQDX interface for intraensemble data network (IEDN) connectivity. The following information is displayed:

IQDX Status
The status of the IQDX interface. See the description of the LnkStatus/IntfStatus field for the possible interface status values.

BytesIn
The number of bytes that have been received over the associated IQDX interface.

Inbound Packets
The number of unicast inbound packets that have been received over the associated IQDX interface.

BytesOut
The number of bytes that have been transmitted over the associated IQDX interface.

Outbound Packets
The number of unicast outbound packets that have been transmitted over the associated IQDX interface.

Associated RNIC Interface

The dynamic interface name that is generated for 10GbE RoCE Express interface that this stack uses for SMC-R communications. This field is

significant only for active IPAQENET and IPAQENET6 interfaces that specify SMCR or take SMCR as the default value.

Associated ISM Interface
The dynamic interface name that is generated for ISM interface that this stack uses for SMC-D communications. This field is significant only for active IPAQENET, IPAQIDIO, IPAQENET6, and IPAQIDIO6 interfaces that specify SMCD or take SMCD as the default value.

SMCR Link Information | SMCD Link Information
The SMCR link information for a RNIC interface or the SMCD link information for an ISM interface. This section is displayed for each RNIC and ISM interface only when the SMC modifier or the SMCID/-U filter is specified. The following fields and statistics are displayed.

Guidelines:

- An SMC-R link is uniquely identified by the combination of the VLAN number, local GID, local VMAC address, local QP number, remote GID, remote VMAC address, and remote QP number.
- An SMC-D link is uniquely identified by the combination of local GID, remote GID, and VLAN number.

LocalSMCLinkId
The SMC-R or SMC-D link identifier that this TCP/IP stack dynamically creates to represent the link.

RemoteSMCLinkId
The SMC-R or SMC-D link identifier that the remote peer uses to represent the link. The value is provided to this TCP/IP stack during link activation.

SMCLinkGroupId
The group identifier that this TCP/IP stack dynamically creates to represent the SMC-R link group that includes this individual link. This value applies to RNIC interfaces only.

VLANid
The virtual LAN ID for this SMC-R or SMC-D link. The value None is displayed if a virtual LAN ID has not been configured.

MTU The negotiated MTU size that is used for this SMC-R link. This value applies to RNIC interfaces only.

LocalGid
The local GID value that is associated with this SMC-R or SMC-D link. This is the same information that is displayed in the `GidAddr` field.

LocalMACAddr
The local virtual MAC address that is associated with this SMC-R link. This value applies to RNIC interfaces only.

LocalQP
The local queue pair (QP) value that is associated with this SMC-R link. This value applies to RNIC interfaces only.

RemoteGid
The peer GID value that is associated with this SMC-R or SMC-D link.

RemoteMACAddr
The peer virtual MAC address that is associated with this SMC-R link. This value applies to RNIC interfaces only.

RemoteQP
The peer QP value that is associated with this SMC-R link. This value applies to RNIC interfaces only.

SMCLinkBytesIn
Number of inbound data bytes transferred across this SMC-R or SMC-D link.

SMCLinkInOperations
Number of ISM inbound operations processed across this SMC-D link, or number of Remote Direct Memory Access (RDMA) inbound operations processed across this SMC-R link.

SMCLinkBytesOut
Number of outbound data bytes transferred across this SMC-R or SMC-D link.

SMCLinkOutOperations
Number of RDMA outbound operations processed across this SMC-R link, or number of ISM outbound operations processed across this SMC-D link.

TCP Connections
Number of TCP connections across this SMC-R or SMC-D link.

Link Receive Buffer Inuse
Amount of memory buffer storage in use by the active TCP connections that are associated with this SMC-R or SMC-D link.

32K Buffer Inuse
Amount of 32K memory buffer storage in use by the active TCP connections that are associated with this SMC-R or SMC-D link.

64K Buffer Inuse
Amount of 64K memory buffer storage in use by the active TCP connections that are associated with this SMC-R or SMC-D link.

128K Buffer Inuse
Amount of 128K memory buffer storage in use by the active TCP connections that are associated with this SMC-R or SMC-D link.

256K Buffer Inuse
Amount of 256K memory buffer storage in use by the active TCP connections that are associated with this SMC-R or SMC-D link.

Other Buffer Inuse
For memory buffer storage that is allocated as buffers larger than 256K, the amount of these other buffers that are in use by the active TCP connections that are associated with this SMC-R or SMC-D link. If no buffers larger than 256K are allocated, this information is not displayed.

Guidelines:

1. The LOOPBACK device and link are displayed. The LOOPBACK6 interface is displayed if the stack is enabled for IPv6.
2. The byte counts for number of bytes received and number of bytes transmitted are always 0 for VIPA links and interfaces.
3. If an MTU was configured on the INTERFACE statement, then the actual MTU is the minimum of the configured MTU and the physical MTU value supported by the interface.

Restrictions:

1. No link-related information, packet trace settings, or BSD parameters are displayed for a device that has no link defined.
2. The packet trace setting is displayed only when it is defined and set to ON.
3. ATM specific information is displayed only for ATM devices that have links defined.

OSA-Express Network Traffic Analyzer Information
This section displays all currently defined OSA interfaces that are dynamically created by VARY TCPIP,,OSAENTA commands or OSAENTA PROFILE statements.

OSA PortName
The port name value of the OSA that is currently defined for performing the OSA-Express network traffic analyzer (OSAENTA) function. This value was specified on the PORTNAME parameter of a VARY TCPIP,,OSAENTA command or on an OSAENTA PROFILE statement. The following information is specific to this *PortName* value.

OSA DevStatus
The device status. The following list shows the possible values:

Starting
An OSAENTA ON command or statement has been processed and TCP/IP has sent an activation request to the data link control (DLC) layer.

Sent SETUP
DLC has acknowledged the TCP/IP activation request and TCP/IP has requested that DLC perform the initial I/O sequence with the device.

Enabling
DLC has acknowledged the TCP/IP activation request and TCP/IP has requested that DLC allow data connections to be established for the device.

Connecting
DLC has accepted the initial I/O sequence request.

Negotiating
The initial I/O sequence with the device is complete and TCP/IP is performing additional link-layer initialization.

Ready The initialization sequence with the device is complete. The device is now ready.

Deactivating
DLC has performed the first stage of an orderly device deactivation.

Not Active
The device is not active. (The device has never been started or has been stopped after having been started.)

OSA IntfName
The name of the interface that is dynamically created to communicate with the OSA Express2 adapter.

OSA IntfStatus
The trace collection interface status. The following list shows the possible values:

Ready The OSA interface used for OSAENTA is accepting all trace requests from the host.

Not Active
The OSA interface that is used for OSAENTA is not active. Either trace collection is disabled or else an error occurred during activation of the OSA interface that is to be used for trace collection. Such an error condition generates an error message on the operator console.

OSA Speed
The speed reported by the interface (in millions of bits per second).

OSA Authorization
The value of the OSA HMC authorization parameter. Possible values are Disabled, Logical Partition, PORT, CHPID, or UNKNOWN. The value is set to UNKNOWN until the first OSAENTA ON command has completed.

Disabled
The OSA does not allow the NTA function to trace any frames for the OSA.

Logical Partition
The OSA allows the NTA function to trace frames only for the current logical partition.

PORT The OSA allows the NTA function to trace frames for all stacks that share this OSA port.

CHPID
The OSA allows the NTA function to trace frames for all stacks that share the OSA.

UNKNOWN
The NTA trace interface has not been activated.

OSAENTA Cumulative Trace Statistics
Statistics accumulated for all frames that have been traced since the OSAENTA interface was first activated. These values are not reset by the OSAENTA ON command or statement.

DataMegs
The number of bytes of trace data (in megabytes) that have been received.

Frames
The total number of frames that have been traced.

DataBytes
The number of bytes of trace data that have been received.

FramesDiscarded
The number of frames that were traced but that the OSA device was not able to either forward to a host image or deliver outbound. These packets are available for formatting in the CTRACE SYSTCPOT component, but have not been delivered to any user.

FramesLost
The number of frames that could not be recorded by TCP/IP in the SYSTCPOT buffers.

OSAENTA Active Trace Statistics
Statistics that have accumulated since the OSAENTA ON command or statement was last issued.

DataMegs
The number of bytes of trace data (in megabytes) that have been collected.

Frames
The total number of frames that have been collected.

DataBytes
The number of bytes of trace data that have been collected.

FramesDiscarded
The number of frames that were collected but that the OSA device was not able to either forward to a host image or deliver outbound. These packets are available for formatting in the CTRACE SYSTCPOT component, but have not been delivered to any user.

FramesLost
The number of frames that were not collected by TCP/IP in the SYSTCPOT buffers.

TimeActive
The number of minutes that have elapsed since the last OSAENTA ON command or statement.

OSAENTA Trace Settings
The current trace settings that are in effect for this OSAENTA interface.

Status The current trace status. Possible values are:

ON Tracing is enabled.

OFF Tracing is disabled.

DataMegsLimit
The amount of data (in megabytes) to be collected before the trace is automatically stopped. This value was specified on the DATA parameter.

FramesLimit
The number of frames to be collected before the trace is automatically stopped. This value was specified on the FRAMES parameter.

TimeLimit
The amount of time (in minutes) that data is collected

before the trace is automatically stopped. This value was specified on the TIME parameter.

Abbrev
The size limit for the frames (in bytes) that are to be traced. This value was specified on the ABBREV parameter. This value can be modified to reflect the size limit set by the OSA.

Discard
Identifies which frames being discarded by the OSA-Express device are to be traced. This value was specified on the DISCARD parameter. Possible values are:

All All frames discarded by the OSA-Express device are traced.

Exception
Frames discarded by the OSA-Express device for exception conditions are traced.

None No discarded frames are traced.

list A list of from one to eight values, that indicate the type of discarded frames that are to be traced by the OSA-Express device. This list includes decimal discard codes and the keyword parameter EXCEPTION.

OSAENTA Trace Filters
The values of the current accumulated filter variables from OSAENTA commands or statements for this OSA. If a filter variable has not been specified using OSAENTA commands or statements, then an asterisk is shown.

Nofilter
The filtering behavior when all filters (DEVICEID, MAC, ETHTYPE, VLANID, IPADDR, PROTOCOL, and PORTNUM) have been cleared or are inactive. This behavior applies when no filters have been specified, if the CLEARFILTER parameter is specified, or when the current setting for every filter is an asterisk (*). This filtering behavior applies only to packets that were not discarded by the OSA-Express device. This value was specified on the NOFILTER parameter. Possible values are:

All All frames are traced.

None No frames are traced.

DeviceID
Up to eight hexadecimal device identifiers that are specified on the DEVICEID keyword of an OSAENTA command or statement. The value is an asterisk (*) if no device identifiers were specified.

Mac Up to eight hexadecimal MAC addresses that are specified on the MAC keyword of an OSAENTA command or statement. The value is an asterisk (*) if no MAC addresses were specified.

VLANid
Up to eight decimal VLAN identifiers that are specified on the VLANID keyword of an OSAENTA command or statement. The value is an asterisk (*) if no VLAN identifiers were specified.

ETHType
Up to eight hexadecimal Ethernet types that are specified on the ETHTYPE keyword of an OSAENTA command or statement. The value is an asterisk (*) if no Ethernet types were specified. The name of the Ethernet type filter is displayed for commonly used Ethernet types, such as ARP, IPv4, IPv6, and SNA.

IPAddr
Up to eight dotted decimal IPv4 IP addresses and up to eight colon hexadecimal IPv6 IP addresses that are specified on the IPADDR keyword of an OSAENTA command or statement. The value is an asterisk (*) if no IP addresses were specified.

Protocol
Up to eight decimal protocol identifiers that are specified on the PROTOCOL keyword of an OSAENTA command or statement. The value is an asterisk (*) if no protocol identifiers were specified. The name of the protocol filter is displayed for commonly used protocols, while the protocol number is displayed for all others.

PORTNum
Up to eight decimal port numbers that are specified on the PORTNUM keyword of an OSAENTA command or statement. The value is an asterisk (*) if no port numbers were specified.

SMCR Link Group Information
The information of the SMC link group. This section is displayed for each RNIC interface only when the SMC modifier or the SMCID/-U filter is specified. The following fields are displayed:

SMCLinkGroupId
The group identifier that this TCP/IP stack dynamically creates to represent the SMC-R link group that includes this individual link.

PNetID
The physical network ID value that is configured in HCD for this SMC-R link group.

Redundancy
The recovery and load balancing capabilities of the link group. The following list shows the possible values:

Full The link group has redundant active SMC-R links. Both the local and remote stacks have full failover capability. The z/OS server performs load balancing of TCP connections across the SMC-R links that are members of the link group.

Partial (Single local internal path)
The link group has redundant active SMC-R links. Both the local and remote stacks have failover capability. The z/OS server performs load balancing of TCP connections across

the SMC-R links that are members of the link group. However, the links on the local stack have the same internal path.

Partial (Single local PCHID, unique ports)
The link group has redundant active SMC-R links. Both the local and remote stacks have failover capability. The z/OS server performs load balancing of TCP connections across the SMC-R links that are members of the link group. However, the links on the local stack have the same PCHID with unique ports.

Partial (Single local PCHID and port)
The link group has redundant active SMC-R links. Both the local and remote stacks have failover capability. The z/OS server performs load balancing of TCP connections across the SMC-R links that are members of the link group. However, the links on the local stack have the same PCHID and port.

Partial (Single local RNIC)
The link group has multiple active SMC-R links and the remote stack has full failover capability, but the local stack has no failover capability. The z/OS server does not perform load balancing of TCP connections.

Partial (Single remote RNIC)
The link group has multiple active SMC-R links and the local stack has full failover capability, but the remote stack has no failover capability. The z/OS server does not perform load balancing of TCP connections.

None (Single local and remote RNIC)
The link group has a single active SMC-R link. Neither the local stack nor the remote stack has failover capability. The z/OS server cannot perform load balancing of TCP connections.

Link Group Receive Buffer Total
Amount of remote memory buffer (RMB) storage that is assigned to this SMC-R link group.

32K Buffer Total
Amount of 32K RMB storage that is assigned to this SMC-R link group.

64K Buffer Total
Amount of 64K RMB storage that is assigned to this SMC-R link group.

128K Buffer Total
Amount of 128K RMB storage that is assigned to this SMC-R link group.

256K Buffer Total
Amount of 256K RMB storage that is assigned to this SMC-R link group.

Other Buffer Total
For RMB storage that is allocated as buffers larger than 256K, the amount of these other buffers that are assigned

to this SMC-R link group. If no buffers larger than 256K are allocated, this information is not displayed.

LocalSMCLinkId
The link identifier this TCP/IP stack dynamically creates to represent the SMC-R link in this SMC-R link group.

RemoteSMCLinkId
The SMC-R link identifier that the remote peer uses to represent the link in this SMC-R link group. The value is provided to this TCP/IP stack during link activation.

PNETID Report Specific Information

Associated
This field is displayed only for ISM and RNIC interfaces. It indicates whether the interface is currently used for SMC communications for the PNETID value that is associated with the interface. The following values are valid:

Yes The interface is currently used for SMC communications for this PNETID.

- If IntfType is RNIC, the interface is used for SMC-R communications. At most two RNIC interfaces can actively be used for a given PNETID.
- If IntfType is ISM, the interface is used for SMC-D communications. The value of Associated is always YES for ISM interfaces.

No The interface is currently not used for SMC-R communications for this PNETID.

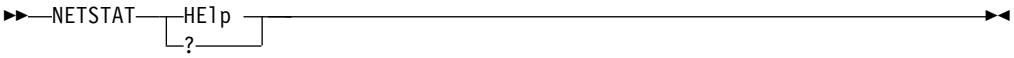
PChid The CHPID value that is associated with this interface.

VChid
The virtual channel ID value that is associated with this interface.

Netstat HElp/-? report

Displays help information for Netstat parameters.

TSO syntax



z/OS UNIX syntax

Command syntax examples

From TSO environment

```
NETSTAT HELP or NETSTAT ?
```

From UNIX shell environment

```
netstat -?
```

Report examples

The following examples are generated by using TSO NETSTAT command. Using the z/OS UNIX **netstat** command displays the data in the same format as the TSO NETSTAT command.

```
NETSTAT HELP or
NETSTAT ?
Usage: NETSTAT <Report option | Command> <Target> <Output> <(Filter>
Report option:
ALL       - Display detailed information about TCP connection
            and UDP sockets
ALLConn   - Display information for all TCP connections and
            UDP sockets, including some recently closed ones
ARp       - Query ARP table or entry information (IPv4 only)
BYTEinfo  - Display the byte-count information for each
            active TCP connection and UDP socket
CACHinfo  - Display information about TCP connections
            utilizing the Cache Accelerator
CLients   - Display information about local users of TCP/IP
            services (jobnames)
CONFIG    - Display the TCP/IP configuration information
COnn      - Display information about each active TCP
            connection and UDP socket (Default option)
DEFADDRT  - Display the policy table for IPv6 default address selection
DEvlinks  - Display information about devices and defined
            interfaces or links
Gate      - Display information about the stack routing table
            for IPv4 destinations
HElp or ? - Display Netstat parameters list
HOme      - Display information about each home IP address
            and its associated link or interface name
IDS       - Display information about Intrusion Detection
            Services
ND        - Display the IPv6 Neighbor cache entries
PORTList  - Display port reservation list
RESCache  - Display resolver cache information
ROUTe     - Display stack routing information
SLAP      - Display QoS policy statistics
SOCKets   - Display information about each client using a
            socket application programming interface
SRCIP     - Displays information for all job-specific source
            VIPA IP address associations
STATS     - Display TCP/IP statistics
TTLS      - Display Application Transparent Transport Layer
            Security (AT-TLS) information
TELnet    - Display TN3270 Telnet server connections
Up        - Date and time tcpip was last started
VCRT      - Display the dynamic VIPA Connection Routing Table
VDPT      - Display the dynamic VIPA Destination Port Table
VIPADCFG  - Display the dynamic VIPA configuration information
VIPADyn   - Display the current dynamic VIPA and VIPAROUTE
            information
Target:
TCP       - Display detailed information about the specified
            TCPIP address space
Output:
FORMat    - Display Netstat report in a given format
REPort    - Netstat information written to dataset name
            tsoprefix.NETSTAT.option or specified with DSN/HLQ
STACk     - Netstat information written to a TSO data stack
```

```
Filter:
APPLD     - Filter the output of ALL,ALLCONN,and CONN reports
            using the specified application data
APPLName  - Filter the output of the TELNET report using the
            specified VTAM application name
CLIent    - Filter the output of ALL, ALLCONN, BYTEINFO, CLIENT,
            CONN, SOCKETS, and TELNET reports using the specified
            client name
CONNType  - Filter the output of ALLCONN and CONN reports using
            the specified connection type
DNSAddr   - Filter the output of RESCACHE using the specified
            DNS IP address.
HOSTNAME  - Filter the output of ALL, ALLCONN, BYTEINFO, CONN, RESCACHE,
            SOCKETS, TELNET and VCRT reports using the specified
            host name
INTFNAME  - Filter the output of DEVLINKS and HOME reports using the
            specified name
IPAddr    - Filter the output of ALL, ALLCONN, BYTEINFO, CONN, GATE,
            ND, RESCACHE, ROUTE, SOCKETS, TELNET, VCRT, VDPT, and VIPADCFG
            reports using the specified IP address
IPPort    - Filter output of the ALL, ALLCONN, CONN, SOCKETS,
            TELNET, VCRT, and VDPT reports using the specified IP
            address and port number
LUName    - Filter the output of the TELNET report using the
            specified LU name
NOTN3270  - Filter the output of ALL, ALLCONN, BYTEINFO, CONN,
            CLIENTS, and SOCKETS reports excluding TN3270 server
            connections
POLicyn   - Filter the output of the SLAP report using the specified
            policy name
POrt      - Filter the output of ALL, ALLCONN, CONN, PORTLIST, SOCKETS,
            TELNET, VCRT, and VDPT reports using the specified port
SMCID   -   Filter the output of ALL, ALLConn, CONN, and DEVLINKS reports
            using the specified SMC-D link, or SMC-R link or SMC-R
            link group identifier
Command:
DRop      - Terminates the socket end-point that is identified by
            the specified connection number
```

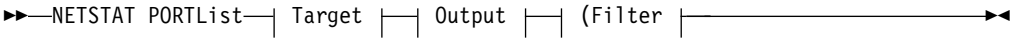
```
netstat -?
Usage: netstat|onetstat <Report Option | Command> <Target> <Output> <Filter>
Report option:
-A  - Display detailed information about TCP connection and UDP
      sockets
-a  - Display information for all TCP connections and UDP sockets,
      including some recently closed ones
-b  - Display the byte-count information for each active TCP
      connection and UDP socket
-C  - Display information about TCP connections utilizing the
      Cache Accelerator
-c  - Display information about each active TCP connection and UDP
      socket (Default option)
-d  - Display information about devices and defined interface or
      links
-e  - Display information about local users of TCP/IP services
      (jobname)
-F  - Display the dynamic VIPA configuration information
-f  - Display the TCP/IP configuration information
-g  - Display information about the stack routing table for IPv4
      destinations
-h  - Display information about each home IP address and its
      associated link or interface name
-J  - Displays information for all job-specific source VIPA IP
      address associations
-j  - Display QoS policy statistics
-k  - Display information about Intrusion Detection Services
-l  - Display the policy table for IPv6 default address selection
-n  - Display the IPv6 Neighbor cache entries
-O  - Display the dynamic VIPA Destination Port Table
-o  - Display port reservation list
-q  - Display resolver cache information
-R  - Query ARP table or entry information (IPv4 only)
-r  - Display stack routing information
-S  - Display TCP/IP statistics
-s  - Display information about each client using socket
      application programming interface
-t  - Display TN3270 Telnet server connections
-u  - Date and time tcpip was last started
-V  - Display the dynamic VIPA Connection Routing Table
-v  - Display the current dynamic VIPA and VIPAROUTE information
-x  - Display Application Transparent Transport Layer
      Security (AT-TLS) information
-?  - Display Netstat parameters list
Target:
-p  - Display detailed information about the specified
      TCPIP address space
Output:
-M  - Display Netstat report in a given format
```

```
Filter:
-B    Filter output of the -A, -a, -c, -s, -t, -O, and -V reports
      using the specified IP address and port number
-E    Filter the output of -A, -a, -b, -c, -e, -s, and -t reports
      using the specified client name
-G    Filter the output of -A, -a, and -c reports using the specified
      application data
-H    Filter the output of -A, -a, -b, -c, -q, -s, -t, and -V reports
      using the specified host name
-I    Filter the output of -A, -a, -b, -c, -F, -g, -n, -q, -r, -s, -t, -O,
      and -V reports using the specified IP address
-K    Filter the output of -d and -h reports using the specified name
-L    Filter the output of -t report using the specified LU name
-N    Filter the output of -t report using the specified application
      name
-P    Filter the output of -A, -a, -c, -s, -t, -O, -o and -V reports
      using the specified port
-Q    Filter the output of -q report using the specified DNS IP address.
-T    Filter the output of -A, -a, -b, -c, -e, and -s reports
      excluding TN3270 server connections
-U    Filter the output of -A, -a, -c, and -d reports using the specified SMC-D link, or
      SMC-R link or SMC-R link group identifier
-X    Filter the output of -a, and -c reports using the specified connection
      type
-Y    Filter the output of -j report using the specified policy name
Command:
-D  - Terminates the socket end-point that is identified by the
      specified connection number
```

Netstat PORTList/-o report

Displays the list of reserved ports and the port access control configuration for unreserved ports. To configure port access control for unreserved ports, replace the port number value with the keyword UNRSV. For more information about port access control see the port access control information in z/OS Communications Server: IP Configuration Guide. For ports that are reserved by the PORTRANGE profile statement, only one output line is displayed for each range. For ephemeral port specifications, see the Netstat CONFIG/-f report description.

TSO syntax



Target

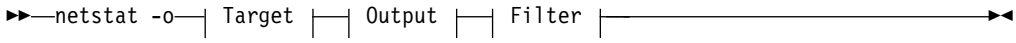
Provide the report for a specific TCP/IP address space by using TCp *tcpname*. See The Netstat command target for more information about the TCp parameter.

Output

The default output option displays the output on the user's terminal. For other options, see “The TSO NETSTAT command syntax” on page 241 or Netstat command output.

Filter

z/OS UNIX syntax



Target

Provide the report for a specific TCP/IP address space by using **-p** *tcpname*. See The Netstat command target for more information about the TCp parameter.

Output

The default output option displays the output to z/OS UNIX shell stdout. For other options, see "The z/OS UNIX netstat command syntax" on page 245 or Netstat command output.

Filter

Filter description

POrt/-P *portnum*
Filter the output of the PORTList/**-O** report using the specified port number *portnum* or the keyword UNRSV. You can enter up to six filter values. The port number range is 1-65535.

Restriction: For a UDP endpoint socket, the filter value only applies to the local or source port.

Command syntax examples

From TSO environment

```
NETSTAT PORTLIST
Display the port reservation list in the default TCP/IP stack.
NETSTAT PORTLIST TCP TCPCS6
Display the port reservation list in the TCPCS6 stack.
```

From UNIX shell environment

```
netstat -o
netstat -o -p tcpcs6
```

Report examples

The following examples are generated by using TSO NETSTAT command. Using the z/OS UNIX **netstat** command displays the data in the same format as the TSO NETSTAT command.

Not IPv6 enabled (SHORT format)

```
NETSTAT PORTLIST MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           15:24:23
Port# Prot User     Flags    Range       IP Address      SAF Name
----- ---- ----     -----    -----       ----------      --------
UNRSV TCP  A*       L
UNRSV TCP  *        FL                                   GENERIC
00020 TCP  FTPD1    D
00021 TCP  FTPD1    DA
00023 TCP  TCPCS    DA
00025 TCP  SMTP     DA
04000 TCP  OMVS     DABU                9.67.113.10
04001 TCP  OMVS     DABFU               9.67.113.12     BS4TOMVS
04004 TCP  *        DAF                                  S4TALL
04005 TCP  *        DABU                9.67.113.11
04017 TCP  *        DABFU               9.67.113.17     BS4TALL
04020 TCP  DCICSTS  DAN
05000 TCP  *        DARN     05000-05001
06020 TCP  *        DAM
06000 TCP  *        DARM     06000-06001
UNRSV UDP  *        XI
00161 UDP  OSNMPD   DA
00162 UDP  OMVS     DA
00514 UDP  SYSLOGD1 DA
04020 UDP  OMVS     DABF                9.67.43.70      BS4UOMVS
04030 UDP  *        DAF                                  S4UALL
05000 UDP  MUD      DAR      05000-05002
```

IPv6 enabled or request for LONG format

```
NETSTAT PORTLIST MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           15:24:23
Port# Prot User     Flags    Range       SAF Name
----- ---- ----     -----    -----       --------
UNRSV TCP  *        FL                   GENERIC
00020 TCP  FTPD1    D
00021 TCP  FTPD1    DA
00023 TCP  TCPCS    DA
00025 TCP  SMTP     DA
04000 TCP  OMVS     DABU
      BindSpecific: 9.67.113.10
04001 TCP  OMVS     DABFU                BS4TOMVS
      BINDSPECIFIC: 9.67.113.12
04002 TCP  OMVS     DABU
      BindSpecific: ::6:2900:1dc:21bc
04020 TCP  DCICSTS  DAN
05000 TCP  *        DARN     05000-05001
06020 TCP  *        DAM
06000 TCP  *        DARM     06000-06001
UNRSV UDP  *        FI                   GENERIC
00514 UDP  SYSLOGD1 DA
04020 UDP  OMVS     DAB
      BindSpecific: 9.67.43.70
04022 UDP  *        DAB
      BindSpecific: 1::8
04030 UDP  *        DA
05000 UDP  MUD      DAR      05000-05002
```

Report field descriptions

Display the following port reservation information defined in the PORT or PORTRANGE profile statements. For more information about each field, see the PORT or PORTRANGE profile statements in the z/OS Communications Server: IP Configuration Reference.

Port#

nnnn For ports reserved by the PORT profile statement, this value is the number of the port that was reserved. For ports that are reserved

by the PORTRANGE profile statement, this value is the number of the first port in the range. Valid values are in the range 1 – 65535.

UNRSV
Indicates any unreserved port; that is, any port number in the range 1-65535 that has not been reserved by a PORT or PORTRANGE statement. For applications that explicitly bind to an unreserved port and match the protocol and *jobname* value on this PORT statement, permission to access the unreserved port is controlled according to the value of the flags for that entry. However, when the RESTRICTLOWPORTS parameter is configured on the TCPCONFIG or UDPCONFIG profile statement, access only to unreserved ports with port numbers greater than 1023 is controlled by the PORT UNRSV statements.

Prot The protocol that was specified in the PORT profile statement. The valid protocol values are TCP and UDP.

User The MVS job name that can use the port. See Client name or User ID descriptions in Netstat report general concepts for detailed descriptions.

Flags The flags represent parameter values defined on the PORT or PORTRANGE profile statement.

A Autolog

B Bind

D DelayAcks

F SAF

I WhenBind

L WhenListen

M Port is explicitly enabled for SMC. For more information about SMC support, see Shared Memory Communications in z/OS Communications Server: IP Configuration Guide.

N Port is explicitly disabled for SMC. For more information about SMC support, see Shared Memory Communications in z/OS Communications Server: IP Configuration Guide.

R Port is reserved by range.

S Share port

U Reuse port. This flag is set for TCP sockets when the BIND keyword is specified (both B and U are set).

W Shareport with WLM server-specific weights is being used.

X Deny

Range This field is significant only for port entry reserved by the PORTRANGE profile statement (flag R in the Flags field).

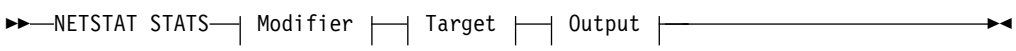
IP address or BindSpecific
This field is significant only for port entries with the BIND parameter specified on the PORT profile statement.

SAF Name
The final qualifier of a security product resource name.

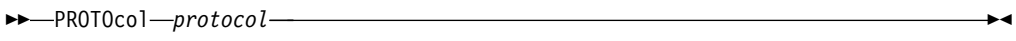
Netstat STATS/-S report

Displays TCP/IP statistics for IP, ICMP, TCP, and UDP protocols. You can use the PROTOCOL filter to display statistics for only a specific protocol.

TSO syntax



Modifier



PROTOcol *protocol*
Display statistics for the specified protocol. The valid protocols are IP, ICMP, TCP, and UDP.

Result: If you specify TCP, you get TCP, SMC-R, and SMC-D statistics. For more information about SMC support, see Shared Memory Communications in z/OS Communications Server: IP Configuration Guide.

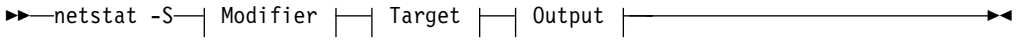
Target

Provide the report for a specific TCP/IP address space by using TCp *tcpname*. See The Netstat command target for more information about the TCp parameter.

Output

The default output option displays the output on the user's terminal. For other options, see "The TSO NETSTAT command syntax" on page 241 or Netstat command output.

z/OS UNIX syntax



Modifier

PROTOcol *protocol*
Display statistics for the specified protocol. The valid protocols are IP, ICMP, TCP, and UDP.

Result: If you specify TCP, you get TCP, SMC-R, and SMC-D statistics. For more information about SMC support, see Shared Memory Communications in the z/OS Communications Server: IP Configuration Guide.

Target

Provide the report for a specific TCP/IP address space by using **-p** *tcpname*. See The Netstat command target for more information about the TCp parameter.

Output

The default output option displays the output to z/OS UNIX shell stdout. For other options, see "The z/OS UNIX netstat command syntax" on page 245 or Netstat command output.

Command syntax examples

From TSO environment

```
NETSTAT STATS
   Provides TCP/IP statistics for IP, ICMP, TCP and UDP protocols.
NETSTAT STATS PROTOCOL IP
   Provides TCP/IP statistics for IP protocol. If the stack is IPv6-enabled, then the
   statistics for IPv6 protocol are also displayed.
NETSTAT STATS PROTOCOL ICMP
   Provides TCP/IP statistics for ICMP protocol. If the stack is IPv6-enabled, then
   the statistics for ICMPv6 protocol are also displayed.
NETSTAT STATS PROTOCOL TCP
   Provides TCP/IP statistics for TCP protocol. If the stack is enabled for SMC-R,
   then the statistics for SMC-R are also displayed. If the stack is enabled for SMC-D,
   then the statistics for SMC-D are also displayed.
NETSTAT STATS PROTOCOL UDP
   Provides TCP/IP statistics for UDP protocol.
```

From UNIX shell environment

```
   netstat -S
   netstat -S PROTOCOL IP
   netstat -S PROTOCOL ICMP
   netstat -S PROTOCOL TCP
   netstat -S PROTOCOL UDP
```

Report examples

The following examples are generated by using TSO NETSTAT command. Using the z/OS UNIX **netstat** command displays the data in the same format as the TSO NETSTAT command.

Not IPv6 enabled (SHORT format)

```
NETSTAT STATS

MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           15:14:15
IP Statistics
  Packets Received                  = 25164
  Inbound Calls from Device Layer   = 12241
  Inbound Frame Unpacking Errors    = 0
  Inbound Discards Memory Shortage  = 0
  Received Header Errors            = 0
  Received Address Errors           = 4961
  Datagrams Forwarded               = 067
  Unknown Protocols Received        = 0
  Received Packets Discarded        = 3
  Received Packets Delivered        = 20203
  Output Requests                   = 8773
  Output Discards No Route          = 0
  Output Discards DLC Sync Errors   = 0
  Output Discards DLC Async Errors  = 0
  Output Discards Memory Shortage   = 0
  Output Discards (other)           = 0
  Reassembly Timeouts               = 0
  Reassembly Required               = 0
  Reassembly Successful             = 0
  Reassembly Failures               = 0
  Datagrams Successfully Fragmented = 0
  Datagrams Failing Fragmentation   = 0
  Fragments Created                 = 0
  Inbound  Packets handled by zIIP  = 12490
  Outbound Packets handled by zIIP  = 4912
```

```
ICMP Statistics
                            Received    Sent
                            --------    ----
  Messages                  1366        7
  Errors                    0           0
  Destination Unreachable   1359        0
  Time Exceeded             0           0
  Parameter Problems        0           0
  Source Quenchs            0           0
  Redirects                 0           0
  Echos                     7           0
  Echo Replies              0           7
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0

TCP Statistics
  Current Established Connections     = 11
  Current Stalled Connections         = 0
  Current Servers In Connection Flood = 0
  Active Connections Opened           = 122
  Passive Connections Opened          = 7
  Connections Closed                  = 78
  Established Connections Dropped     = 8
  Connection Attempts Dropped         = 4
  Connection Attempts Discarded       = 2
  Timewait Connections Reused         = 0
  Segments Received                   = 10900
  Header Prediction Ok for ACK        = 1643
  Header Prediction Ok for Data       = 3213
  Duplicate ACKs                      = 134
  Discards for Bad Checksum           = 0
  Discards for Bad Header Length      = 0
  Discards for Data too Short         = 9
  Discards for Old Timestamp          = 2
  Segments Completely Duplicate       = 23
  Segments Partially Duplicate        = 4
  Segments Completely After Window    = 0
  Segments Partially After Window     = 0
  Segments Out of Order               = 43
  Segments Received After Close       = 2
  Window Probes Received              = 5
  Window Updates Received             = 9
  Segments Received on OSA Bulk Queues= 9
  Segments Sent                       = 8382
  Window Updates Sent                 = 723
  Delayed ACKs Sent                   = 43
  Resets Sent                         = 4
  Segments Retransmitted              = 21
  Retransmit Timeouts                 = 0
  Connections Dropped by Retransmit   = 0
  Path MTU Discovery Retransmits      = 0
  Path MTU Beyond Retransmit Limit    = 0
  Window Probes Sent                  = 2
  Connections Dropped during Probe    = 0
  KeepAlive Probes Sent               = 0
  Connections Dropped by KeepAlive    = 0
  Connections Dropped by Finwait2     = 0
  Configured Ephemeral Ports          = 200
  Configured Ephemeral Ports In Use   = 5
  Configured Ephemeral Ports Max Usage= 5
  Ephemeral Ports Exhausted           = 0
```

```
SMCD Statistics
  Current Established SMC Links       = 2
  Active SMC Links Opened              = 4
  Passive SMC Links Opened             = 0
  SMC Links Closed                     = 2
  Current Established Connections      = 1
  Active Connections Opened            = 1
  Passive Connections Opened           = 0
  Connections Closed                   = 0
  Segments Received                    = 1
  Segments Sent                        = 1
  Resets Sent                          = 0
  Resets Received                      = 0
SMCR Statistics
  Current Established SMC Links       = 2
  SMC Link Activation Time Outs        = 0
  Active SMC Links Opened              = 4
  Passive SMC Links Opened             = 0
  SMC Links Closed                     = 2
  Current Established Connections      = 1
  Active Connections Opened            = 1
  Passive Connections Opened           = 0
  Connections Closed                   = 0
  Segments Received                    = 1
  Segments Sent                        = 1
  Resets Sent                          = 0
  Resets Received                      = 0
UDP Statistics
  Datagrams Received    = 6984
  No Port Errors        = 2312
  Receive Errors        = 0
  Datagrams Sent        = 368
  Configured Ephemeral Ports          = 200
  Configured Ephemeral Ports In Use   = 6
  Configured Ephemeral Ports Max Usage= 7
  Ephemeral Ports Exhausted           = 0
```

NETSTAT STATS PROTOCOL IP

```
MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           15:14:15
IP Statistics
  Packets Received                  = 25164
  Inbound Calls from Device Layer   = 12241
  Inbound Frame Unpacking Errors    = 0
  Inbound Discards Memory Shortage  = 0
  Received Header Errors            = 0
  Received Address Errors           = 4961
  Datagrams Forwarded               = 067
  Unknown Protocols Received        = 0
  Received Packets Discarded        = 3
  Received Packets Delivered        = 20203
  Output Requests                   = 8773
  Output Discards No Route          = 0
  Output Discards DLC Sync Errors   = 0
  Output Discards DLC Async Errors  = 0
  Output Discards Memory Shortage   = 0
  Output Discards (other)           = 0
  Reassembly Timeouts               = 0
  Reassembly Required               = 0
  Reassembly Successful             = 0
  Reassembly Failures               = 0
  Datagrams Successfully Fragmented = 0
  Datagrams Failing Fragmentation   = 0
  Fragments Created                 = 0
  Inbound  Packets handled by zIIP  = 12490
  Outbound Packets handled by zIIP  = 4912
```

```
NETSTAT STATS PROTOCOL ICMP

MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           15:14:15
ICMP Statistics
                              Received    Sent
                              --------    ----
  Messages                    1366        7
  Errors                      0           0
  Destination Unreachable     1359        0
  Time Exceeded               0           0
  Parameter Problems          0           0
  Source Quenchs              0           0
  Redirects                   0           0
  Echos                       7           0
  Echo Replies                0           7
  Timestamps                  0           0
  Timestamp Replies           0           0
  Address Masks               0           0
  Address Mask Replies        0           0
```

IPv6 enabled or request for LONG format

```
NETSTAT STATS

MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           15:14:15
IP Statistics (IPv4)
  Packets Received                    = 34
  Received Header Errors              = 0
  Received Address Errors             = 3
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 3
  Received Packets Delivered          = 46
  Output Requests                     = 31
  Output Discards No Route            = 0
  Output Discards (other)             = 0
  Reassembly Timeouts                 = 0
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0
  Inbound  Packets handled by zIIP    = 12490
  Outbound Packets handled by zIIP    = 4912
IPv6 Statistics
  Packets Received                    = 0
  Received Header Errors              = 0
  Received Address Errors             = 0
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 0
  Received Packets Delivered          = 0
  Output Requests                     = 0
  Output Discards No Route            = 0
  Output Discards (other)             = 0
  Reassembly Timeouts                 = 0
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0
  Inbound  Packets handled by zIIP    = 0
  Outbound Packets handled by zIIP    = 0
IP General Statistics
  Inbound Calls from Device Layer     = 91
  Inbound Frame Unpacking Errors      = 0
  Inbound Discards Memory Shortage    = 0
  Output Discards DLC Sync Errors     = 0
  Output Discards DLC Async Errors    = 0
  Output Discards Memory Shortage     = 0
```

```
ICMP Statistics (IPV4)
                            Received    Sent
                            --------    ----
  Messages                  12          12
  Errors                    0           12
  Destination Unreachable   12          12
  Time Exceeded             0           0
  Parameter Problems        0           0
  Source Quenchs            0           0
  Redirects                 0           0
  Echos                     0           0
  Echo Replies              0           0
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0
ICMPv6 Statistics
                            Received    Sent
                            --------    ----
  Messages                  0           4
  Errors                    0           0
  Destination Unreachable   0           0
  Time Exceeded             0           0
  Parameter Problems        0           0
  Redirects                 0           0
  Echos                     0           0
  Echo Replies              0           0
  Administratively Prohibited 0         0
  Packet Too Big            0           0
  Router Solicitations      0           0
  Router Advertisements     0           0
  Neighbor Solicitations    0           0
  Neighbor Advertisements   0           0
  Group Membership Queries  0           0
  Group Membership Responses 0          4
  Group Membership Reductions 0         0
```

```
TCP Statistics
  Current Established Connections     = 2
  Current Stalled Connections         = 0
  Current Servers In Connection Flood = 0
  Active Connections Opened           = 1
  Passive Connections Opened          = 1
  Connections Closed                  = 0
  Established Connections Dropped     = 0
  Connection Attempts Dropped         = 0
  Connection Attempts Discarded       = 0
  Timewait Connections Reused         = 0
  Segments Received                   = 6
  Header Prediction Ok for ACK        = 0
  Header Prediction Ok for Data       = 2
  Duplicate ACKs                      = 0
  Discards for Bad Checksum           = 0
  Discards for Bad Header Length      = 0
  Discards for Data too Short         = 0
  Discards for Old Timestamp          = 0
  Segments Completely Duplicate       = 0
  Segments Partially Duplicate        = 0
  Segments Completely After Window    = 0
  Segments Partially After Window     = 0
  Segments Out of Order               = 0
  Segments Received After Close       = 0
  Window Probes Received              = 0
  Window Updates Received             = 0
  Segments Received on OSA Bulk Queues= 9
  Segments Sent                       = 7
  Window Updates Sent                 = 0
  Delayed ACKs Sent                   = 2
  Resets Sent                         = 0
  Segments Retransmitted              = 0
  Retransmit Timeouts                 = 0
  Connections Dropped by Retransmit   = 0
  Path MTU Discovery Retransmits      = 0
  Path MTU Beyond Retransmit Limit    = 0
  Window Probes Sent                  = 0
  Connections Dropped during Probe    = 0
  KeepAlive Probes Sent               = 0
  Connections Dropped by KeepAlive    = 0
  Connections Dropped by Finwait2     = 0
  Configured Ephemeral Ports          = 200
  Configured Ephemeral Ports In Use   = 5
  Configured Ephemeral Ports Max Usage= 5
  Ephemeral Ports Exhausted           = 0
```

```
SMCD Statistics
  Current Established SMC Links       = 2
  Active SMC Links Opened              = 4
  Passive SMC Links Opened             = 0
  SMC Links Closed                     = 2
  Current Established Connections      = 1
  Active Connections Opened            = 1
  Passive Connections Opened           = 0
  Connections Closed                   = 0
  Segments Received                    = 1
  Segments Sent                        = 1
  Resets Sent                          = 0
  Resets Received                      = 0
SMCR Statistics
  Current Established SMC Links       = 2
  SMC Link Activation Time Outs        = 0
  Active SMC Links Opened              = 4
  Passive SMC Links Opened             = 0
  SMC Links Closed                     = 2
  Current Established Connections      = 1
  Active Connections Opened            = 1
  Passive Connections Opened           = 0
  Connections Closed                   = 0
  Segments Received                    = 1
  Segments Sent                        = 1
  Resets Sent                          = 0
  Resets Received                      = 0

UDP Statistics
  Datagrams Received    = 0
  No Port Errors        = 12
  Receive Errors        = 0
  Datagrams Sent        = 12
  Configured Ephemeral Ports          = 200
  Configured Ephemeral Ports In Use   = 6
  Configured Ephemeral Ports Max Usage= 7
  Ephemeral Ports Exhausted           = 0
```

```
NETSTAT STATS PROTOCOL IP

MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           15:14:15
IP Statistics (IPv4)
  Packets Received                    = 34
  Received Header Errors              = 0
  Received Address Errors             = 3
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 3
  Received Packets Delivered          = 46
  Output Requests                     = 31
  Output Discards No Route            = 0
  Output Discards (other)             = 0
  Reassembly Timeouts                 = 0
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0
  Inbound  Packets handled by zIIP    = 12490
  Outbound Packets handled by zIIP    = 4912
IPv6 Statistics
  Packets Received                    = 0
  Received Header Errors              = 0
  Received Address Errors             = 0
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 0
  Received Packets Delivered          = 0
  Output Requests                     = 0
  Output Discards No Route            = 0
  Output Discards (other)             = 0
  Reassembly Timeouts                 = 0
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0
  Inbound  Packets handled by zIIP    = 0
  Outbound Packets handled by zIIP    = 0
IP General Statistics
  Inbound Calls from Device Layer     = 91
  Inbound Frame Unpacking Errors      = 0
  Inbound Discards Memory Shortage    = 0
  Output Discards DLC Sync Errors     = 0
  Output Discards DLC Async Errors    = 0
  Output Discards Memory Shortage     = 0
```

```
NETSTAT STATS PROTOCOL ICMP

MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPCS           15:14:15
ICMP Statistics (IPV4)
                              Received    Sent
                              --------    ----
  Messages                    12          12
  Errors                      0           12
  Destination Unreachable     12          12
  Time Exceeded               0           0
  Parameter Problems          0           0
  Source Quenchs              0           0
  Redirects                   0           0
  Echos                       0           0
  Echo Replies                0           0
  Timestamps                  0           0
  Timestamp Replies           0           0
  Address Masks               0           0
  Address Mask Replies        0           0
ICMPv6 Statistics
                              Received    Sent
                              --------    ----
  Messages                    0           4
  Errors                      0           0
  Destination Unreachable     0           0
  Time Exceeded               0           0
  Parameter Problems          0           0
  Redirects                   0           0
  Echos                       0           0
  Echo Replies                0           0
  Administratively Prohibited 0           0
  Packet Too Big              0           0
  Router Solicitations        0           0
  Router Advertisements       0           0
  Neighbor Solicitations      0           0
  Neighbor Advertisements     0           0
  Group Membership Queries    0           0
  Group Membership Responses  0           4
  Group Membership Reductions 0           0
```

Report field descriptions

Most of the TCP/IP statistics for IP, ICMP, TCP, and UDP protocols are defined in the SNMP IP-MIB (RFC2011 - *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2*), TCP-MIB (RFC 2012 - *SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2*), and UDP-MIB (RFC 2013 - *SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2*) MIB modules. See these SNMP MIB modules for more detailed information.

- The following describes the IPv4 and IPv6 statistics displayed:

  Packets Received
  The total number of input datagrams received from interfaces.

  Received Header Errors
  The number of input datagrams discarded due to errors in their IP headers.

  Received Address Errors
  The number of input datagrams discarded because the IP address in their IP header's destination field was not valid.

  Datagrams Forwarded
  The number of input datagrams forwarded to their final destination.

  Unknown Protocols Received
  The number of datagrams discarded because of an unknown or unsupported protocol.

Received Packets Discarded
The number of input datagrams that were discarded that are not accounted for in another input discard counter.

Received Packets Delivered
The total number of input datagrams successfully delivered to IP user-protocols.

Output Requests
The total number of IP datagrams that local IP user-protocols supplied to IP in requests for transmission.

Output Discards No Route
The number of IP datagrams discarded because no route could be found to transmit them to their destination.

Output Discards (Other)
The number of output datagrams generated by this stack that could not be transmitted.

Reassembly Timeouts
The number of packets that were being held for reassembly but which were discarded due to the fact that the remaining fragments were not received within reassembly timeout.

Reassembly Required
The number of IP fragments received that needed to be reassembled.

Reassembly Successful
The number of IP datagrams successfully reassembled.

Reassembly Failures
The number of failures detected by the IP reassembly algorithm.

Datagrams Successfully Fragmented
The number of IP datagrams that have been successfully fragmented.

Datagrams Failing Fragmentation
The number of IP datagrams that have been discarded because they needed to be fragmented but could not be.

Fragments Created
The number of IP datagram fragments that have been generated as a result of fragmentation.

Inbound Packets handled by zIIP
The number of inbound packets that were processed by a zIIP. This counter applies only to IPSec workloads, whose CPU cycles are being displaced to a zIIP. The Packets Received counter includes the packets that are received on zIIP, so the percentage of total inbound packets that were processed by zIIP can be calculated as (Inbound Packets handled by zIIP ÷ Packets Received) × 100. Similarly, the number of inbound packets that were processed by General Purpose Processors is equal to (Packets Received - Inbound Packets handled by zIIP).

Outbound Packets handled by zIIP
The number of outbound packets that were processed by a zIIP. This counter applies only to IPSec workloads, whose CPU cycles are being displaced to a zIIP. The Output Requests counter includes the outbound packets processed on zIIP, so the percentage of total outbound packets that were processed by zIIP can be calculated as (Outbound Packets handled by zIIP ÷ Output Requests) × 100. Similarly, the number of

outbound packets that were processed by General Purpose Processors is equal to (Output Requests - Outbound Packets handled by zIIP).

- The following describes the IP general statistics displayed. The statistic values for these counters reflect both IPv4 and IPv6 processing combined.

  Inbound Calls from Device Layer
  The number of times the inbound TCP/IP Data Path has received control from the Device Layer.

  Inbound Frame Unpacking Errors
  The number of times a received frame could not be unpacked into its constituent datagrams.

  Inbound Discards Memory Shortage
  The number of inbound packets discarded due to a CSM storage shortage condition.

  Output Discards DLC Sync Errors
  The number of outbound packets discarded due to a synchronous error in the Data Link Control.

  Output Discards DLC Async Errors
  The number of outbound packets discarded due to an asynchronous error in the Data Link Control.

  Output Discards Memory Shortage
  The number of outbound packets discarded due to a CSM storage shortage condition.

- The following describes the ICMP statistics displayed:

  Messages
  The total number of ICMP messages received and sent.

  Errors The number of ICMP messages received and sent but determined as having ICMP-specific errors.

  Destination Unreachable
  The number of ICMP Destination Unreachable messages received and sent.

  Time Exceeded
  The number of ICMP Time Exceeded messages received and sent.

  Parameter Problems
  The number of ICMP Parameter Problem messages received and sent.

  Source Quenchs
  The number of ICMP Source Quench messages received and sent.

  Redirects
  The number of ICMP Redirect messages received and sent.

  Echos The number of ICMP Echo (request) messages received and sent.

  Echo Replies
  The number of ICMP Echo Reply messages received and sent.

  Timestamps
  The number of ICMP Timestamp (request) messages received and sent.

  Timestamp Replies
  The number of ICMP Timestamp Reply messages received and sent.

Address Masks
The number of ICMP Address Mask (request) messages received and sent.

Address Mask Replies
The number of ICMP Address Mask Reply messages received and sent.

- The following describes the ICMPv6 statistics displayed:

  Messages
  The total number of ICMPv6 messages received and sent.

  Errors The number of ICMPv6 messages received and sent but determined as having ICMPv6-specific errors.

  Destination Unreachable
  The number of ICMPv6 Destination Unreachable messages received and sent.

  Time Exceeded
  The number of ICMPv6 Time Exceeded messages received and sent.

  Parameter Problems
  The number of ICMPv6 Parameter Problem messages received and sent.

  Redirects
  The number of ICMPv6 Redirect messages received and sent.

  Echos The number of ICMPv6 Echo messages received and sent.

  Echo Replies
  The number of ICMPv6 Echo Reply messages received and sent.

  Administratively Prohibited
  The number of ICMPv6 Administratively Prohibited messages received and sent.

  Packet Too Big
  The number of ICMPv6 Packet Too Big messages received and sent.

  Router Solicitations
  The number of ICMPv6 Router Solicitation messages received and sent.

  Router Advertisements
  The number of ICMPv6 Router Advertisement messages received and sent.

  Neighbor Solicitations
  The number of ICMPv6 Neighbor Solicitation messages received and sent.

  Neighbor Advertisements
  The number of ICMPv6 Neighbor Advertisement messages received and sent.

  Group Membership Queries
  The number of ICMPv6 Group Membership Queries received and sent.

  Group Membership Responses
  The number of ICMPv6 Group Membership Responses received and sent.

  Group Membership Reductions
  The number of ICMPv6 Group Membership Reductions received and sent.

- The following describes the TCP statistics displayed:

  Current Established Connections
  The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

  Guideline: This value, when displayed for TCP statistics, includes the number of TCP connections across SMC-R and SMC-D links. To determine the number of TCP connections that are not across SMC-R links, subtract the value for `Current Established Connections` displayed under `SMCR Statistics` from this value. To determine the number of TCP connections that are not across SMC-D links, subtract the value for `Current Established Connections` displayed under `SMCD Statistics` from this value.

  Current Stalled Connections
  The number of TCP connections whose send data flow is stalled. The send data flow is considered stalled if one or more of the following conditions are true:
  - The TCP send window size is less than 256 or is less than the smaller of the largest send window that has been seen for the connection and the default MTU. The TCP send window size is set based on values provided by the TCP peer. The default MTU for IPv4 is 576. The default MTU for IPv6 is 1280.
  - The TCP send queue is full and the data is not being retransmitted.

  Current Servers In Connection Flood
  The number of TCP servers under a potential connection flood attack. A server is considered under a potential connection flood attack when backlog queue expansion is required to handle the incoming connection requests. When more than 25 servers are under a potential connection flood attack, no server's backlog queue will be allowed to expand.

  Active Connections Opened
  The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

  Guideline: This value, when displayed for TCP statistics, includes the number of TCP connections across SMC-R and SMC-D links that made a direct transition to the SYN-SENT state from the CLOSED state. To determine the number of these TCP connections that are not across SMC-R links, subtract the value for `Active Connections Opened` displayed under `SMCR Statistics` from this value. To determine the number of these TCP connections that are not across SMC-D links, subtract the value for `Active Connections Opened` displayed under `SMCD Statistics` from this value.

  Passive Connections Opened
  The number of times that TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state. This value, when displayed for TCP statistics, includes the number of TCP connections across SMC-R and SMC-D links that made a direct transition to the SYN-RCVD state from the LISTEN state. To determine the number of the TCP connections that are not across SMC-R links, subtract the value for `Passive Connections Opened` displayed under `SMCR Statistics` from this value. To determine the number of the TCP connections that are not across SMC-D links, subtract the value for `Passive Connections Opened` displayed under `SMCD Statistics` from this value.

Connections Closed
Number of TCP connections that have corresponding sockets closed.

Guideline: This value, when displayed for TCP statistics, includes the number of TCP connections across SMC-R and SMC-D links that have corresponding sockets closed. To determine the number of these TCP connections that are not across SMC-R links, subtract the value for `Connections Closed` displayed under `SMCR Statistics` from this value. To determine the number of these TCP connections that are not across SMC-D links, subtract the value for `Connections Closed` displayed under `SMCD Statistics` from this value.

Established Connections Dropped
The number of times TCP connections made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state. This value includes the number of TCP connections across SMC-R links.

Connection Attempts Dropped
The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the listen state from the SYN-RCVD state.

Connection Attempts Discarded
Number of passive connection requests discarded.

Timewait Connections Reused
Number of TCP connections in the TIMEWAIT state that have been reused for connections in the SYN-RCVD state.

Segments Received
The total number of segments received.

Guideline: This value, when displayed for TCP statistics, includes the number of Remote Direct Memory Access (RDMA) inbound operations that are processed across all SMC-R and SMC-D links. To determine the number of segments that are received on TCP connections that do not traverse SMC-R links, subtract the value for `Segments Received` displayed under `SMCR Statistics` from this value. To determine the number of segments that are received on TCP connections that do not traverse SMC-D links, subtract the value for `Segments Received` displayed under `SMCD Statistics` from this value.

Segments Received on OSA Bulk Queues
The total number of segments received for all connections from the BulkData ancillary input queue (AIQ) of the OSA-Express QDIO inbound workload queueing function. For more information about QDIO inbound workload queueing, see z/OS Communications Server: IP Configuration Guide.

Header Prediction Ok for ACK
Number of inbound TCP acknowledgments with successful header prediction.

Header Prediction Ok for Data
Number of inbound TCP data segments with successful header prediction.

Duplicate ACKs
Number of inbound duplicate TCP acknowledgments.

Discards for Bad Checksum
Number of inbound TCP segments discarded due to bad checksum.

Discards for Bad Header Length
Number of inbound TCP segments discarded due to bad header length.

Discards for Data too Short
Number of inbound TCP segments discarded due to data length shorter than segment length.

Discards for Old Timestamp
Number of inbound TCP segments discarded due to old timestamp.

Segments Completely Duplicate
Number of inbound TCP segments with all data before current TCP window.

Segments Partially Duplicate
Number of inbound TCP segments with some data before current TCP window.

Segments Completely After Window
Number of inbound TCP segments with all data after current TCP window.

Segments Partially After Window
Number of inbound TCP segments with some data after current TCP window.

Segments Out of Order
Number of inbound TCP segments that did not contain the next expected sequence number.

Segments Received After Close
Number of inbound TCP segments received after corresponding sockets have been closed.

Window Probes Received
Number of inbound TCP segments processed while current receive window size is 0.

Window Updates Received
Number of inbound TCP segments that only change receive window size.

Segments Sent
The total number of segments sent.

Guideline: This value, when displayed for TCP statistics, includes the number of RDMA outbound operations that are processed across all SMC-Rand SMC-D links. To determine the number of segments that were sent on TCP connections that do not traverse SMC-R links, subtract the value for `Segments Sent` displayed under `SMCR Statistics` from this value. To determine the number of segments that were sent on TCP connections that do not traverse SMC-D links, subtract the value for `Segments Sent` displayed under `SMCD Statistics` from this value.

Window Updates Sent
Number of outbound TCP segments that only change receive window size.

Delayed ACKs Sent
Number of delayed outbound TCP acknowledgments.

Resets Sent
Number of TCP segments sent containing the RST flag.

Guideline: This value, when displayed for TCP statistics, includes the number of TCP connections that were using SMC-R and SMC-D links. To determine the number of these segments that were sent for TCP connections that were not using SMC-R links, subtract the value for `Resets Sent` displayed under `SMCR Statistics` from this value. To determine the number of these segments that were sent for TCP connections that were not using SMC-D links, subtract the value for `Resets Sent` displayed under `SMCD Statistics` from this value.

Segments Retransmitted
The total number of segments retransmitted.

Retransmit Timeouts
Number of TCP retransmit timer pops.

Connections Dropped by Retransmit
Number of TCP connections dropped due to retransmit threshold exceeded.

Path MTU Discovery Retransmits
Number of outbound TCP segments retransmitted due to path MTU discovery.

Path MTU Beyond Retransmit Limit
Number of TCP connections that exceeded path MTU discovery retransmit threshold.

Window Probes Sent
Number of outbound window probe requests.

Connections Dropped during Probe
Number of TCP connections dropped due to no response while sending window probe requests.

KeepAlive Probes Sent
Number of keepalive probe requests. This value includes the number of TCP connections across SMC-R links.

Connections Dropped by KeepAlive
Number of TCP connections dropped because of no response when sending keepalive probe requests. This value includes the number of TCP connections across SMC-R links.

Connections Dropped by Finwait2
Number of TCP connections dropped because of FINWAIT2 timer expiring before receiving FIN segments. This value includes the number of TCP connections across SMC-R links.

Configured Ephemeral Ports
Number of configured ephemeral ports to be assigned for TCP applications.

Ephemeral Ports In Use
The number of ephemeral ports currently in use by TCP applications.

Ephemeral Ports Max Usage
The highest number of ephemeral ports in use by TCP applications at any time.

Ephemeral Ports Exhausted
The number of times a bind() request failed because all available ephemeral ports were in use.

- The following describes the SMC-D statistics that are displayed:

Current Established SMC Links
The current number of active SMC-D links.

Active SMC Links Opened
The number of times that an SMC-D link was established and this stack acted in the server role during link establishment.

Passive SMC Links Opened
The number of times that an SMC-D link was established and this stack acted in the client role during link establishment.

SMC Links Closed
The number of SMC-D links that were closed.

Current Established Connections
The number of TCP connections over SMC-D links for which the current state is either ESTABLISHED or CLOSE-WAIT.

Active Connection Opened
The number of times that TCP connections over SMC-D links made a direct transition to the SYN-SENT state from the CLOSED state.

Passive Connection Opened
The number of times that TCP connections over SMC-D links made a direct transition to the SYN-RCVD state from the LISTEN state.

Connections Closed
The number of TCP connections over SMC-D links that have corresponding sockets closed.

Segments Received
The number of SMC-D inbound operations that were processed across all SMC-D links.

Segments Sent
The number of SMC-D outbound operations that were processed across all SMC-D links.

Resets Sent
The number of SMC-D outbound operations that contained the abnormal close flag. This flag is set when the connection is abnormally terminated. For example, the TCP connection was Reset.

Resets Received
The number of SMC-D inbound operations that contained the abnormal close flag. This flag is set when the connection is abnormally terminated. For example, the TCP connection was Reset.

- The following describes the SMC-R statistics that are displayed:

Current Established SMC Links
The current number of active SMC-R links.

SMC Link Activation Time Outs
The number of times that an attempt occurred to establish an SMC-R link, but the attempt failed because of timeout conditions.

Active SMC Links Opened
The number of times that an SMC-R link was established and this stack acted in the server role during link establishment.

Passive SMC Links Opened
The number of times that an SMC-R link was established and this stack acted in the client role during link establishment.

SMC Links Closed
The number of SMC-R links that were closed.

Current Established Connections
The number of TCP connections over SMC-R links for which the current state is either ESTABLISHED or CLOSE-WAIT.

Active Connection Opened
The number of times that TCP connections over SMC-R links made a direct transition to the SYN-SENT state from the CLOSED state.

Passive Connection Opened
The number of times that TCP connections over SMC-R links made a direct transition to the SYN-RCVD state from the LISTEN state.

Connections Closed
The number of TCP connections over SMC-R links that have corresponding sockets closed.

Segments Received
The number of SMC-R inbound operations that were processed across all SMC-R links.

Segments Sent
The number of SMC-R outbound operations that were processed across all SMC-R links.

Resets Sent
The number of SMC-R outbound operations that contained the abnormal close flag. This flag is set when the connection is abnormally terminated. For example, the TCP connection was Reset.

Resets Received
The number of SMC-R inbound operations that contained the abnormal close flag. This flag is set when the connection is abnormally terminated. For example, the TCP connection was Reset.

- The following describes the UDP statistics displayed:

Datagrams Received
The total number of UDP datagrams delivered to UDP users.

No Port Errors
The total number of received UDP datagrams for which there was no application at the destination port.

Receive Errors
The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

Datagrams Sent
The total number of UDP datagrams sent.

Configured Ephemeral Ports
Number of configured ephemeral ports to be assigned for UDP applications.

Ephemeral Ports In Use
The number of ephemeral ports currently in use by UDP applications.

Ephemeral Ports Max Usage
The highest number of ephemeral ports in use by UDP applications at any time.

Ephemeral Ports Exhausted
The number of times a bind() request failed because all available ephemeral ports were in use.

z/OS UNIX and TSO Netstat option comparison

The following table shows the equivalent z/OS UNIX and TSO command formats.

Table 14. z/OS UNIX and TSO Netstat command options

TSO option	z/OS UNIX option	Description
Report Options		
ALL	**-A**	Displays detailed information about TCP connections and UDP sockets, including some recently closed ones.
ALLConn	**-a**	Displays information for all TCP connections and UDP sockets, including some recently closed ones.
ARp	**-R**	Displays ARP cache information.
BYTEinfo	**-b**	Displays the byte-count information for each active TCP connection and UDP socket.
CACHinfo	**-C**	Displays statistics for TCP listening sockets uszing the Fast Response Cache Accelerator (FRCA).
CLients	**-e**	Displays information about local users of TCP/IP services (jobnames).
CONFIG	**-f**	Displays the TCP/IP configuration information.
COnn	**-c**	Displays the information about each active TCP connection and UDP socket.
DEFADDRT	**-l**	Displays the policy table for IPv6 default address selection.
DEvlinks	**-d**	Displays information about interfaces that are defined to the TCP/IP stack.
Gate	**-g**	Displays information about the stack routing table for IPv4 destinations.
HElp	-?	Displays help information for Netstat parameters.
Home	**-h**	Displays information about each home IP address and its associated link or interface name.
IDS	**-k**	Displays information about Intrusion Detection Services. Displays Neighbor Discovery cache information (IPv6 only).
ND	**-n**	Displays Neighbor Discovery cache information (IPv6 only).
PORTList	**-o**	Displays the reserved port list.
RESCACHE	**-q**	Displays resolver cache information
ROUTe	**-r**	Displays information about the stack routing table for IPv4 destinations and IPv6 destinations if stack is IPv6 enabled.

Table 14. z/OS UNIX and TSO Netstat command options (continued)

TSO option	z/OS UNIX option	Description
SLAP	**-j**	Displays QoS Policy statistics.
SOCKets	**-s**	Displays the information about each client using a socket application programming interface.
SRCIP	**-J**	Displays the configured information for all job-specific, source IP address designations on the target TCP/IP.
STATS	**-S**	Displays TCP/IP statistics for IP, ICMP, TCP and UDP protocols.
TELnet	**-t**	Displays information for TN3270 Telnet server connections.
TTLS	**-x**	Displays Application Transparent Transport Layer Security (AT-TLS) information.
Up	**-u**	Displays the date and time that TCP/IP was started and specifies whether it is IPv6 enabled or disabled.
VCRT	**-V**	Displays the dynamic VIPA Connection Routing Table used for sysplex distributor and moveable dynamic VIPA support.
VDPT	**-O**	Displays the dynamic VIPA Distribution Port Table information.
VIPADCFG	**-F**	Displays the dynamic VIPA configuration for a TCP/IP stack.
VIPADyn	**-v**	Displays the current dynamic VIPA and VIPAROUTE information for a TCP/IP stack.
Target		
TCp	**-p**	Displays information for a specified TCP/IP address space.
Output		
FORMat	**-M**	Displays Netstat report in a given format.
REPort	n/a	Causes the output to be stored in the data set userid.NETSTAT.option.
STACk	n/a	Causes the output to be placed in the TSO data stack.
Filter		
APPLD	**-G**	Filter the output of ALL/**-A**, ALLConn/**-a**, and COnn/**-c** reports using the application data.
APPLname	**-L**	Filter the output of the TELnet/**-t** report using the specified VTAM application name.
CLIent	**-E**	Filter the output of the ALL/**-A**, ALLConn/**-a**, BYTEinfo/**-b**, CLient/**-e**, COnn/**-c**, SOCKets/**-s**, and TELnet/**-t** reports using the specified client name.
CONNType	**-X**	Filter the output of the ALLConn/**-a** and COnn/**-c** reports using the specified connection type.
DNSAddr	**-Q**	Filter the output of the RESCache/**-q** report using the specified DNS IP address.
HOSTName	**-H**	Filter the output of the ALL/**-A**, ALLConn/**-a**, BYTEinfo/**-b**, COnn/**-c**, RESCache/**-q**, SOCKets/**-s**, TELnet/**-t**, and VCRT/**-V** reports using the specified host name.
INTFName	**-K**	Filter the output of the DEvlinks/**-d** and HOme/**-h** reports using the specified interface name.
IPAddr	**-I**	Filter the output of the ALL/**-A**, ALLConn/**-a**, BYTEinfo/**-b**, COnn/**-c**, Gate/**-g**, ND/**-n**, RESCache/**-q**, ROUTe/**-r**, SOCKets/**-s**, TELnet/**-t**, VCRT/**-V**, VDPT/**-O**, and VIPADCFG/**-F** reports using the specified IP address.

Table 14. z/OS UNIX and TSO Netstat command options (continued)

TSO option	z/OS UNIX option	Description
IPPort	**-B**	Filter the output of the ALL/**-A**, ALLConn/**-a**, COnn/**-c**, SOCKets/**-s**, TELnet/**-t**, VCRT/**-V**, and VDPT/**-O** reports using the specified IP address and port number.
LUName	**-L**	Filter the output of the TELnet/**-t** report using the specified LU name.
NOTN3270	**-T**	Filter the output of the ALL/**-A**, ALLConn/**-a**, BYTEinfo/**-b**, CLient/**-e**, COnn/**-c**, and SOCKets/**-s** reports excluding TN3270 server connections.
POLicyn	**-Y**	Filter the output of the SLAP/**-j** report using the specified policy rule name.
POrt	**-P**	Filter the output of the ALL/**-A**, ALLConn/**-a**, COnn/**-c**, PORTList/**-o**, SOCKets/**-s**, TELnet/**-t**, VCRT/**-V**, and VDPT/**-O** reports using the specified port number.
SMCID	**-U**	Filter the output of the ALL/**-A**, ALLConn/**-a**, COnn/**-c**, and DEvlinks/**-d** reports using the specified SMC-R link, SMC-R link group, or SMC-D link identifier.
Command		
DRop	**-D**	Terminates the socket end-point that is identified by the specified connection number.

Chapter 7. IP and SNA Codes

Data link control (DLC) status codes

DLC status codes provide information about errors that are encountered during the use of high performance data transfer (HPDT) services. They are displayed in some messages and in the IUTx VIT entry.

DLC status codes are 4 bytes long. The bytes contain the following information:

Byte **Contents**

0 Category

1 Reporting layer identifier and location

2 and 3
Completion code

The following tables show the possible values that can appear in each byte and their meaning.

Table 15. Byte 0 (category) of the DLC status code

Hexadecimal Value	Meaning
X'00'	Request successful **Explanation:** The specific primitive has been processed with no error. The receiver of this primitive successfully forwarded or replied to this primitive successfully. **Note:** The completion code could have informational errors.
X'08'	Request rejected **Explanation:** All aspects of the primitive were understood but a transitory system or network error occurred which prevented the execution of this request. An example of this could be storage shortage. **Note:** This category is one that an upper layer protocol (ULP) might choose to try the failed primitive again.
X'10'	Request error **Explanation:** This primitive was rejected due to inaccurate information in the primitive (for example, incorrect token, incorrect information element).
X'20'	State error **Explanation:** A primitive was received “out of order.”
X'40'	Usage error **Explanation:** Primitive rejected due to incorrect use of either the primitive itself or a parameter that is associated with the primitive.
X'80'	Permanent error **Explanation:** Request rejected due to failure of either a system or network function.

Table 16. Byte 1 (reporting layer identifier and location) of the DLC status code

Hexadecimal Value	Meaning
X'10'	LLC layer local error **Explanation:** A primitive was processed and an error was found by the local VTAM.
X'20'	LLC layer path error **Explanation:** A primitive was processed and an error was found by the local VTAM while trying to send a primitive out on an MPC group.
X'30'	LLC layer remote error **Explanation:** A primitive was processed and an error was found by the remote VTAM. This value should be used when a remote VTAM is sending common status back to an adjacent host.
X'12'	Port Control Manager (PCM) local error **Explanation:** A primitive was processed and an error was found by the IBM Open System Adapter's PCM.
X'22'	Port Control Manager path-related error **Explanation:** A primitive was processed and an error was found by the IBM Open System Adapter's PCM while trying to send a primitive out on an MPC group or sending a primitive to the ATM network.
X'32'	Port Control Manager remote error **Explanation:** A primitive was processed and an error was found by the remote node; for example, the local ATM switch experienced a failure.
X'1C'	Service-specific component local error **Explanation:** A primitive was processed and an error was found by a service-specific component part of the ATM adaptation layer (AAL) sublayer.
X'2C'	Service-specific component path-related error **Explanation:** A primitive was processed and an error was found by a service-specific component part of the AAL sublayer, while trying to send a primitive to the ATM network.
X'3C'	Service-specific component remote error **Explanation:** A primitive was processed and an error was found by the remote node; for example, the local ATM switch experienced a failure.
X'1A'	Common-part component local error **Explanation:** A primitive was processed and an error was found by a common-part component that includes the ATM layer function and non-service-specific sublayers of the AAL layer.
X'2A'	Common-part component path-related error **Explanation:** A primitive was processed and an error was found by a common-part component that includes the ATM layer function and non-service-specific sublayers of the AAL layer while trying to send a primitive to the ATM network.
X'3A'	Common-part component remote error **Explanation:** A primitive was processed and an error was found by a remote partner in its common-part component that includes the ATM layer function and non-service-specific sublayers of the AAL layer.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code

Hexadecimal Code	Meaning
X'00nn'	n/a **Explanation:** Codes starting with X'00' are specific to the VTAM product implementation.
X'0000'	Successful **Explanation:** The primitive completed successfully.
X'0001'	Initialization failure **Explanation:** A failure occurred during the initialization of support code. Notify VTAM operator to determine cause of failure.
X'0018'	VTAM is not available **Explanation:** Request returned as a result of VTAM termination. Termination might be normal due to an operator initiated action or due to some abnormal condition.
X'0021'	Connection constructor error **Explanation:** Failure occurred during the construction of the connection object. Notify the VTAM operator of the failure to determine cause and possible corrective actions.
X'0022'	State error **Explanation:** Failure occurred during the execution of the request due to a state error indicating a protocol violation. Notify the VTAM operator of the failure to determine cause of inconsistency and possible corrective actions.
X'0023'	TRLE activation/deactivation state error **Explanation:** User issued an activate or deactivation request and an internal state error was encountered.
X'0024'	Provider ID error **Explanation:** Provider ID supplied on the primitive is either incorrect or cannot be found. Condition indicates an interface inconsistency. Notify the VTAM operator of the failure to determine cause of inconsistency and possible corrective actions.
X'0025'	Selective Retransmit Not Supported **Explanation:** A request to set up a connection was received, and Selective Retransmit service was requested for that connection. Selective Retransmit is not supported now, so the request was rejected. Condition indicates that the remote partner expects Selective Retransmit, which might be a configuration mismatch. Notify the VTAM operator of the failure to determine cause of inconsistency and possible corrective actions.
X'0027'	OpenPathReq error **Explanation:** Internal command OPENPATH_request, which causes the initial activation of the channel paths and either the XID or IDX exchange, failed. Failure might be due to a channel problem or an error condition that is discovered during the initial activation sequence. Notify the VTAM operator of the failure to determine cause and possible corrective actions. It might also be necessary to notify the operator of the platform containing the remote MPC instance.
X'0029'	DactPathReq error **Explanation:** Internal command DACTPATH_request, which causes the termination of an MPC group, failed for some reason. MPC will complete system takedown of the group but the user should notify the VTAM operator of the failure to determine cause and possible corrective actions. Failure to take corrective action might lead to the inability to reactivate the path.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'002A'	ActPathRsp error **Explanation:** Internal command ACTPATH_response, which causes the allocation of devices and the construction of the MPC environment, failed. Notify the VTAM operator of the failure to determine cause and possible corrective actions.
X'002B'	OpenPathRsp error **Explanation:** Internal command OPENPATH_response, which causes the initial activation of the channel paths and either the XID or IDX exchange, failed. Failure might be due to a channel problem or an error condition that is discovered during the initial activation sequence. Notify the VTAM operator of the failure to determine cause and possible corrective actions. It might also be necessary to notify the operator of the platform containing the remote MPC instance.
X'002F'	MPC connection does not support high performance data transfer. **Explanation:** Either the local definitions or the remote partner does not support high performance data transfer data interface. Check Hardware Configuration Definition (HCD) and VTAM definitions for possible mismatch.
X'0030'	Storage error **Explanation:** Storage incorrect or not obtainable.
X'0040'	INOP-deact SAP **Explanation:** SAP becomes inoperative.
X'0041'	INOP-connection **Explanation:** Data connection becomes inoperative.
X'0042'	INOP-signaling connection **Explanation:** Signaling connection becomes inoperative.
X'0043'	INOP-device **Explanation:** Local device becomes inoperative.
X'0044'	INOP-soft **Explanation:** The connection or MPC group is inoperative; however, recovery of the connection is possible.
X'0045'	INOP-hard **Explanation:** The connection or MPC group is inoperative, and is not expected to recover without intervention.
X'0046'	Incorrect token **Explanation:** User specified an incorrect token on a data connection.
X'0047'	Incorrect token **Explanation:** Internally specified token incorrect.
X'0048'	Duplicate data activation request **Explanation:** ULP has sent multiple data activation requests for a single connection.
X'0049'	Selector value error **Explanation:** A primitive was processed that specified a selector that did not match the selector of the provider token that was received.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'004A'	Protocol value error **Explanation:** A primitive was processed that did not specify a known protocol value.
X'004B'	VCNAME value error **Explanation:** A primitive was processed that did not specify a known virtual circuit value.
X'0050'	Multiple TCP/IP instances trying to register filters for incoming calls **Explanation:** Multiple TCP/IPs requested identical filter values.
X'0051'	Buffer size error **Explanation:** An activation SAP request was issued with an incorrect bufsize, or an incorrect combination of buffer size and buffer number for a TCP/IP read or write device.
X'0052'	Missing XBFL **Explanation:** An attempt was made to execute a data primitive and an XBFL (extended buffer list) was not provided. An XBFL is required for data primitives.
X'0053'	Empty XBFL **Explanation:** An XBFL was provided for a data primitive that has no entries within the list; for example, XBFLBEGN=0.
X'0054'	Incorrect XBFL entry **Explanation:** An XBFL was provided for a data primitive that has an incorrect entry within the list (for example, XBFLAREA=0).
X'0055'	Packet and XBFL length mismatch **Explanation:** An XBFL was provided for a data primitive where the total length of all entries does not match the packet length.
X'0056'	XBFL free option not specified **Explanation:** An XBFL was provided for a data primitive where the XBFL free option (XBFL_FREE_OPT) was not specified. The free option is required for all data primitives.
X'0057'	Incorrect packet length **Explanation:** The packet length was 0 or too large; for example, exceeds the defined values for the device.
X'0058'	Incorrect parameter list version **Explanation:** The parameter list version is incorrect.
X'0060'	Connection not active **Explanation:** The data activation request for a specific connection was received before the connection was active.
X'0061'	Data not enabled with data activation request **Explanation:** Data activation request has not been received so data cannot be processed.
X'0062'	Class value error **Explanation:** A primitive was processed that does not specify a known class value.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'0063'	Control value error **Explanation:** A primitive was processed that does not specify a known control value which is permitted for this primitive.
X'0064'	MPC Group in Use **Explanation:** An MPC group is defined as EXCLUSIVE USE (MPCUSAGE = EXC on TRLE), and is already in use. Activation is rejected.
X'0065'	iQDIO Prohibited **Explanation:** iQDIO activation is prohibited by VTAM start option IQDCHPID = NONE.
X'0066'	iQDIO CHPID Ambiguous **Explanation:** iQDIO activation is not allowed due to an ambiguous configuration with specifying IQDCHPID = ANY (default), and configuring (HCD/IOCDS) multiple IQD CHPIDs to this logical partition (LPAR). When IQDCHPID = ANY is specified (or defaulted) only one IQD CHPID can be configured for this LPAR. If multiple IQD CHPIDs must be configured to this LPAR, then define IQDCHPID = 'HEXCHPID' (the specific hex IQDCHPID that this LPAR should use).
X'0067'	iQDIO or QDIO Devices Not Available **Explanation:** An attempt was made to build a dynamic TRLE for a QDIO OSA-Express device or a HiperSockets device, but VTAM could not find the minimum number of required subchannel devices (CUAs) for the device. For a HiperSockets device, at least 3 CUAs are required to the same HiperSockets CHPID. For a QDIO OSA-Express device, the OSA-Express CHPID must be configured with 2 consecutive device addresses beginning with an even number for the control channels, and at least one additional device address for a DATAPATH channel. Verify the HCD or IOCDS configuration for accuracy for this logical partition (LPAR).
X'0068'	iQDIO CHPID Conflict **Explanation:** The user defined an iQDIO device CHPID and it conflicts with the sysplex IQD CHPID. This is defined by the IQDCHPID start option and is used for DYNAMICXCF communication. For more information, see the IQDCHPID start option in z/OS Communications Server: SNA Resource Definition Reference.
X'0069'	Processor not iQDIO capable **Explanation:** The user attempted to activate an iQDIO device and the processor does not support iQDIO devices.
X'006A'	iQDIO IQD CHPID multiple channel subsystem error **Explanation:** Multiple channel subsystem capable machine but the Internal Channel ID (CHID) is not available.
X'006B'	Frame invalidation mismatch **Explanation:** Frame invalidation is not supported by the stack that is issuing ActSap and frame invalidation was enabled by the first stack to issue ActSap.
X'006C'	Too many input queues requested by the stack **Explanation:** The stack specified more input queues than supported.
X'006D'	Input queue ID out of range **Explanation:** An internal Communications Server error occurred.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'006E'	Input queue ID not registered **Explanation:** An internal Communications Server error occurred.
X'006F'	QDIO or IQDIO CHPID Not Available **Explanation:** An attempt was made to build a dynamic TRLE for a QDIO OSA-Express device or a HiperSockets device, and a CHPID for this device could not be found. If the CHPID was configured, for example on an MPCIPA HiperSockets device statement or using the CHPID parameter on an OSA-Express QDIO Interface statement, that particular CHPID was not defined to the system. If the CHPID was searched for dynamically, for example activating a dynamic IUTIQDIO link for HiperSockets with VTAM start option IQDCHPID=ANY or an OSA-Express OSM device, a CHPID for that particular channel type was not defined to the system. Verify the configured CHPID parameter or the HCD or IOCDS configuration for accuracy for this logical partition (LPAR).
X'0070'	QDIO device control channels not available **Explanation:** An attempt was made to build a dynamic TRLE for a QDIO OSA-Express device. A CHPID was found, but two consecutively numbered device addresses beginning with an even number could not be found. For QDIO OSA-Express devices, an even-numbered device address is required for the READ control channel, and the next consecutive odd address for the WRITE control channel. Verify the HCD or IOCDS configuration for accuracy for this logical partition (LPAR).
X'30nn'	n/a **Explanation:** Codes starting with X'30' can be errors that are detected in the interface between TCP/IP and VTAM, between VTAM and the IBM Open System Adapter, or between VTAM and TCP/IP channel units. These errors result from either a software or definitional problem. Use the specific return code to help identify the problem.
X'3001'	Incorrect control information field **Explanation:** The control information field of the primitive contains data that is blank, in an incorrect format, or cannot be recognized.
X'3002'	Incorrect identifier **Explanation:** The value that is specified in the identifier/token parameter of the control information field is blank, in an incorrect format, or cannot be recognized.
X'3003'	Incorrect identifier type **Explanation:** The value that is specified in the identifier type parameter of the control information field is incorrect; for example, the ID type says it is an SAP but the identifier is a filter.
X'3004'	Incorrect primitive **Explanation:** The value that is specified in the primitive code parameter of the control information field is incorrect.
X'3005'	State error **Explanation:** An illogical or incorrect primitive was received for the current SAP or the call instance state of the Port Connection Manager.
X'3007'	Incorrect information data **Explanation:** Either the primitive's data information field is missing data, or it contains blank, syntactically incorrect, or unrecognizable data.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'3008'	Resource not available **Explanation:** The requested resource is not available.
X'300A'	Task ABEND **Explanation:** An error occurred that prevents the processing of the primitive.
X'300E'	Incorrect service type **Explanation:** The ServiceType parameter in the primitive's Control Information field is either blank, syntactically incorrect, or unrecognizable. Service Type is REQ/CNF/IND/RSP.
X'3011'	IBM Open Systems Adapter disabled **Explanation:** The IBM Open Systems Adapter has been disabled by user command.
X'3012'	PVC removed from IBM Open Systems Adapter **Explanation:** A PVC definition has been removed from IBM Open Systems Adapter while that PVC connection was active. The PVC connection is being deactivated.
X'3013'	PCM signaling virtual channel is not active **Explanation:** The signaling virtual channel (VCI=5, VPCI=0) between the IBM Open Systems Adapter and the ATM switch that carries signaling requests is not active.
X'3014'	Incorrect entry point **Explanation:** The entry point/interpret routine indicated contains a null character or incorrect value.
X'3016'	Incorrect Port Control Manager name **Explanation:** The value that is specified in the Port Control Manager name parameter is blank, in an incorrect format, or cannot be recognized. **Note:** 1. The port name is specified in multiple places and **MUST** be the same in the IBM Open Systems Adapter/SF configuration file, on the PORTNAME operand on the TRLE definition statement in the TRL major node, and (in the case of APPN communication) on the PORTNAME operand on the PORT definition statement in the XCA major node. The port name must be the same in all places that it is specified. If it is not, correct the mismatches. 2. The user request is failed if the requested TRLE cannot be activated because of one of the following conditions. • TRL major node has not been activated. • The TRLE entry is missing from the activated TRL major node. • The TRLE entry has an error that does not allow it to be defined. • The TRLE has been activated but it is inoperative.
X'3017'	Incorrect user call instance identifier **Explanation:** The value that is specified in the user call instance identifier parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.
X'3018'	Incorrect provider call instance identifier **Explanation:** The value that is specified in the provider call instance identifier parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'3019'	Incorrect user SAP identifier **Explanation:** The value that is specified in the user SAP identifier parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.
X'301A'	Incorrect provider SAP identifier **Explanation:** The value that is specified in the provider SAP identifier parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.
X'301B'	Incorrect provider call enabling identifier **Explanation:** The value that is specified in the P_CE_ID parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.
X'301C'	Incorrect user call enabling identifier **Explanation:** The value that is specified in the U_CE_ID parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.
X'3022'	Incorrect control information field length **Explanation:** The value that is specified in the control information field length parameter contains an incorrect value. **Note:** Each primitive has a unique fixed control information field.
X'3023'	Incorrect data information field length **Explanation:** The value that is specified in the data information field length parameter contains a value that is incorrect or unrecognized.
X'3024'	Incorrect action code **Explanation:** The value that is specified in the action code specified in the control information on the Call_Setup response field is missing, blank, in an incorrect format, or cannot be recognized.
X'3025'	Missing data information field **Explanation:** The data information field must be complete for the primitive to work.
X'3026'	Incorrect logical link value **Explanation:** The value that is specified in the logical link identifier parameter is outside the valid range of 0-31, decimal.
X'3027'	PCM TRLE cannot support selector **Explanation:** The user issued an activate request that specified a selector that is not valid for the TRLE found by RNAME.
X'3028'	Datapath device activation failed **Explanation:** A storage error occurred during early processing of a datapath channel address for a QDIO device.
X'3029'	Datapath device activation negative **Explanation:** An error occurred attempting to allocate or activate a datapath channel address for a QDIO device.
X'302A'	Datapath device Open failed **Explanation:** An error occurred attempting to start a connection across a datapath channel address for a QDIO device.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'302B'	Datapath Device Start Data failed **Explanation:** An error occurred attempting to start data flow on a connection across a datapath channel address for a QDIO device.
X'302C'	Enable Incoming connections for Port failed **Explanation:** A QDIO device rejected an attempt to allow connections to be enabled on this device.
X'302D'	No datapath devices available **Explanation:** A ULP cannot use a QDIO device because there are no datapath channel addresses available.
X'302E'	Activation failed to complete **Explanation:** A QDIO or iQDIO device failed to complete activation or properly register its HOME IP Address within 5 minutes.
X'302F'	Channel unit address not available **Explanation:** The channel is not the correct type for this device, there is no path for this channel, or the channel is not varied online.
X'3030'	Incorrect channel unit address specification **Explanation:** The channel unit address was either not specified by TCP/IP or is not a correct hexadecimal number.
X'3031'	Channel unit address already in use **Explanation:** The channel unit address specified by TCP/IP is already allocated to another user.
X'3032'	Maximum connections exceeded **Explanation:** The connection request attempted for this device exceeds the allowable maximum for this device type.
X'3033'	Lack of resources **Explanation:** The resources requested from the system could not be obtained (for example, memory errors).
X'3034'	Connection failed by the remote host with no cause code **Explanation:** A connection request was failed by the remote host for a given device, but a cause code indicating why the connection failed was not supplied.
X'3035'	QDIO CHPID type mismatch **Explanation:** An attempt was made to activate a QDIO device for a particular CHPID type, but the TRLE associated with this device was already active with channels of a different CHPID type. Verify the DEVICE name or PORTNAME are correctly configured for this device, and if the TRLE was configured, verify the device addresses are addresses for a CHPID of the correct type.
X'3036'	Secondary OSM Interface activated before primary **Explanation:** An attempt was made to activate EZ6OSM02 before EZ6OSM01. This failure can occur when there are no OSM CHPIDs available at TCP/IP stack initialization, and EZ6OSM02 is subsequently activated before EZ6OSM01. Activate EZ6OSM01 then EZ6OSM02.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'3037'	OSX or OSM Interface activation not permitted **Explanation:** An attempt was made to activate an interface with CHPID type OSX or OSM. The activation attempt failed because the ENSEMBLE start option is set to NO, which does not permit TCP/IP connectivity to either the intraensemble data network or the intranode management network.
X'3038'	OSX or OSM Interface activation not permitted **Explanation:** An attempt was made to activate an interface with CHPID type OSX or OSM. The activation attempt failed because the central processor complex (CPC) is not configured as a member of an ensemble.
X'3039'	IQD activation not permitted against an IQDX device **Explanation:** A CHPID that is defined to HCD as IQDX cannot be used as an iQDIO device.
X'303A'	Function type not valid **Explanation:** The IBM 10GbE RoCE Express interface does not recognize the function identifier on the activation attempt.
X'303B'	Outbound request flood detected **Explanation:** The Internet Control Message Protocol (ICMP) time stamp request is rejected because CSM storage is constrained or too many time stamp requests are generated at the same time.
X'3053'	Maximum number of network interfaces exceeded **Explanation:** An attempt was made to activate an OSA-Express port in QDIO mode. The OSA-Express port, or another port on the same OSA-Express3 or later channel path identifier (CHPID), is currently operating in optimized latency mode for at least one network interface. Optimized latency mode limits the number of concurrent network interfaces allowed to share this port and this CHPID. This activation attempt exceeds that limit. See the information about the optimized latency mode in z/OS Communications Server: IP Configuration Guide for information about these limits.
X'31nn'	OSA-Express rejected an attempt to activate a port **Explanation:** Codes starting with X'31' are specific to OSA-Express QDIO Mode activation attempts. X'31' indicates that the OSA has rejected an activation attempt. The *nn* indicates the reason for the rejection. Specific *nn* codes are listed in this table. If you receive a code that is not listed in this table, contact IBM Service.
X'311B'	Duplicate port name **Explanation:** An attempt was made to activate an OSA-Express3 or later port in QDIO mode. The port name for this activation attempt was already in use on the other port that belongs to that CHPID. Two ports on the same CHPID cannot have the same port name.
X'3150'	Incorrect port name **Explanation:** An attempt was made to activate an OSA-Express port in QDIO mode. The port name for this activation attempt did not match the port name already assigned to this port by a previous user. All z/OS users of that port must activate with the same port name.
X'32nn'	n/a **Explanation:** Codes starting with X'32' are specific to ATM connection establishment. In particular, they relate to the inability of the IBM Open Systems Adapter to establish a reserved bandwidth connection because of lack of available resources.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'3201'	Bytes per second exceeded **Explanation:** The IBM Open Systems Adapter received a request for a reserved bandwidth circuit. The number of bytes per second that were requested cannot be honored because the IBM Open Systems Adapter's capacity for bytes per second for reserved bandwidth connections would be exceeded.
X'3202'	Receive packets per second exceeded **Explanation:** The IBM Open Systems Adapter received a request for a reserved bandwidth circuit. The number of packets per second that were requested in the receive direction (to the IBM Open Systems adapter) cannot be honored because the IBM Open Systems Adapter's capacity for receive packets per second for reserved bandwidth connections would be exceeded.
X'3203'	Transmit packets per second exceeded **Explanation:** The IBM Open Systems Adapter received a request for a reserved bandwidth circuit. The number of packets per second that were requested in the transmit direction (from the IBM Open Systems Adapter) cannot be honored because the IBM Open Systems Adapter's capacity for transmit packets per second for reserved bandwidth connections would be exceeded.
X'3204'	No packet buffers available **Explanation:** The IBM Open Systems Adapter received a request for a reserved bandwidth circuit. The number of bytes per second that were requested cannot be honored because the IBM Open Systems Adapter's capacity for packet buffers for reserved bandwidth connections would be exceeded.
X'3205'	Bandwidth unavailable **Explanation:** The IBM Open Systems Adapter received a request for a reserved bandwidth circuit. The number of ATM cells per second that were requested cannot be honored because the total number of cells per second would exceed the physical capacity of the ATM link.
X'3210'	Network down **Explanation:** The IBM Open Systems Adapter has lost communications to the ATM switch to which it is attached. The OSA lost communication with the attached ATM network, or an attempt was made to activate an XCA while the OSA had lost communication with the network (a missing cable or a switch registration failure, for example.)
X'33nn'	n/a **Explanation:** Codes starting with X'33' are specific to ATM signaling or data transfer. Generally they are the result of either a ULP software or definitional problem in constructing an ATM primitive. Use the specific return code to identify incorrect parameter, termed an information element (IE), to perform diagnostics.
X'330B'	Call does not exist **Explanation:** The Port Control Manager received a primitive associated with a call that no longer or never existed.
X'330D'	Endpoint does not exist **Explanation:** The value of the endpoint reference identifier in the endpoint reference subfield is not currently assigned to a call endpoint.
X'3312'	Service access point not activated **Explanation:** The primitive is incorrect because the SAP is not activated or recognized.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'3315'	User subfields too large **Explanation:** The subfields specified in the primitive exceed the number of allowable octets.
X'331B'	Subfields not allowed **Explanation:** The subfields contained in the specified primitive are not allowed.
X'331D'	Mandatory subfield missing **Explanation:** A required subfield not present.
X'3323'	Selected channel busy **Explanation:** The specified permanent virtual channel (PVC) is busy or allocated to another call.
X'3324'	Maximum calls exceeded **Explanation:** The call setup request was not executed because the required resource could not be allocated.
X'3329'	Maximum requests exceed **Explanation:** The limit on outstanding primitives was reached.
X'332A'	Call clear indication pending **Explanation:** A call clear indicate has been issued to the user. The user should respond. The call instance is cleared when the call clear response is received from the user.
X'332D'	Timeout on call **Explanation:** The call could not be processed within the time constraints of the network.
X'332F'	Lack of resources **Explanation:** The resources requested from the system (for example, memory errors) could not be obtained.
X'3330'	Operating system error **Explanation:** An operating system error was encountered.
X'3331'	Incorrect bearer capability **Explanation:** The length or the parameter information in the bearer capability subfield is incorrect.
X'3332'	Incorrect channel identification **Explanation:** The length or the parameter information in the channel identification subfield is incorrect or the channel not varied online properly by operator.
X'3333'	Incorrect calling party number **Explanation:** The length or the parameter information in the calling party number subfield is incorrect.
X'3334'	Incorrect called party number **Explanation:** The length or the parameter information in the called party number subfield is incorrect.
X'3335'	Incorrect calling party subaddress **Explanation:** The length or the parameter information in the calling party aubaddress subfield is incorrect.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'3336'	Incorrect called party subaddress **Explanation:** The length or the parameter information in the called party subaddress subfield is incorrect.
X'3337'	Incorrect low-layer compatibility **Explanation:** The length or the parameter information in the low-layer compatibility subfield is incorrect.
X'3338'	Incorrect high-layer compatibility **Explanation:** The length or the parameter information in the high-layer compatibility subfield is incorrect.
X'3339'	Incorrect transit network selection **Explanation:** The length or the parameter information in the transit network selection subfield is incorrect.
X'333A'	Incorrect cause **Explanation:** The length or the parameter information in the cause subfield is incorrect.
X'333B'	Incorrect call status **Explanation:** The length or the parameter information in the call status subfield is incorrect.
X'333C'	No cause code specified **Explanation:** The incoming call clearing message from the network did not contain a cause code indicating why the call was being cleared.
X'3340'	Incorrect AAL parameters **Explanation:** The length or parameter values in the AAL parameters subfield is incorrect.
X'3341'	Duplicate AAL parameters **Explanation:** The AAL parameters subfield is specified more than once.
X'3342'	Incorrect endpoint identifier **Explanation:** The length or parameter value in the endpoint reference subfield is incorrect.
X'3343'	Duplicate endpoint reference **Explanation:** The endpoint reference is specified more than once.
X'3344'	Incorrect endpoint state **Explanation:** The length or parameter value in the endpoint status subfield is incorrect.
X'3346'	Incorrect QoS **Explanation:** The length or parameter values in the quality of service subfield is incorrect.
X'3347'	Duplicate QoS **Explanation:** The quality of service subfield is specified more than once.
X'3348'	Incorrect PCI **Explanation:** The length or the parameter value in the permanent connection identifier subfield is incorrect.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'3349'	Duplicate PCI **Explanation:** The permanent connection identifier subfield is specified more than once.
X'334A'	Incorrect traffic descriptor **Explanation:** The length or the parameter value in the traffic descriptor subfield is incorrect.
X'334B'	Duplicate traffic descriptor **Explanation:** The traffic descriptor subfield is specified more than once.
X'3351'	Duplicate bearer capability **Explanation:** The bearer capability subfield was specified more than one time.
X'3352'	Duplicate channel identification **Explanation:** The channel identification subfield was specified more than one time.
X'3353'	Duplicate calling party number **Explanation:** The calling party number subfield was specified more than one time.
X'3354'	Duplicate called party number **Explanation:** The called party number subfield was specified more than one time.
X'3355'	Duplicate calling party subaddress **Explanation:** The calling party subaddress subfield was specified more than one time.
X'3356'	Duplicate called party subaddress **Explanation:** The called party subaddress subfield was specified more than one time.
X'3357'	Too many instances of low-layer information **Explanation:** More instances of low-layer information subfield are present than are allowed.
X'3358'	Duplicate high-layer compatibility **Explanation:** The high-layer compatibility subfield was specified more than one time.
X'3359'	Duplicate Transit network selection **Explanation:** The transit network selection subfield was specified more than one time.
X'335A'	Duplicate cause **Explanation:** The cause subfield was specified more than one time.
X'335B'	Duplicate call status **Explanation:** The call status subfield was specified more than one time.
X'335D'	Duplicate PCI **Explanation:** The permanent connection identifier subfield was specified more than one time.
X'3360'	Subfield of length zero present **Explanation:** One of the subfields in the data information field has a length of zero.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'3361'	Incorrect calling party number length **Explanation:** In the calling party number subfield, the value that is specified in the SFNumberLength parameter disagrees with the length of the subfield contained in the SFLength parameter.
X'3362'	Incorrect called party number length **Explanation:** In the called party number subfield, the value that is specified in the SFNumberLength parameter disagrees with the length of the subfield contained in the SFLength parameter.
X'3363'	Incorrect calling party subaddress length **Explanation:** In the calling party subaddress subfield, the value that is specified in the SFSubaddrLength parameter disagrees with the length of the subfield contained in the SFLength parameter.
X'3364'	Incorrect called party subaddress length **Explanation:** In the called party subaddress subfield, the value that is specified in the SFSubaddrLength parameter disagrees with the length of the subfield contained in the SFLength parameter.
X'3366'	Incorrect call status value **Explanation:** In the call status subfield, the SFCallStatus parameter specifies a value that is incorrect.
X'3367'	Call status subfield missing **Explanation:** The call status subfield information is missing. This is required information for this primitive.
X'336A'	Subfields of the same type are not the same **Explanation:** Two or more subfields of the same type are specified in the data information field; however they are not contiguous.
X'336B'	Entry not unique **Explanation:** The filter registration request is rejected because the call routing information and subfield specifications indicated in the data information field do not make the entry unique. An entry exists in the Port Control Manager incoming call routing table that has the same “must match” information as this request.
X'336C'	First subfield is not primitive specific **Explanation:** The first subfield you specified in the data information field is not the primitive-specific subfield.
X'3371'	Path Control Manager internal error **Explanation:** The Path Control Manager associated with the call detected an internal error.
X'3374'	Permanent connection not defined **Explanation:** The permanent connection that was requested in the call setup request is not defined.
X'3375'	Incorrect ID type in current state **Explanation:** In the current state of the call instance, the identifier type is incorrect.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'3376'	Call setup confirm for unsuccessful call queued **Explanation:** The Path Control Manager will not process this call clear request because the call that the user requested to be cleared failed.
X'337A'	Prior call control request outstanding **Explanation:** A call control request previously issued by the user has not been confirmed by the Path Control Manager. The user should try the request again after the confirmation is received from the Path Control Manager.
X'3380'	User software error **Explanation:** The user discovered an unexpected software error.
X'3393'	Incorrect usage indicator in primitive-specific subfield **Explanation:** The usage indicator provided in the primitive specific subfield on the filter registration request primitive is incorrect. Either the first primitive-specific subfield specified must meet the “must not match” criteria, or the second primitive-specific subfield specified must meet the “must match” criteria.
X'3394'	Incorrect called party address in filter registration request or data transmission flow control state is blocked. **Explanation:** If this error occurs during device activation, the called party number on the filter registration request is incorrect; either it was not supplied, or does not match an address registered to the Path Control Manager. Otherwise a halt data flow request has been sent so data is not flowing.
X'3395'	Connection state incorrect for data transfer **Explanation:** Data cannot be accepted until the data SAP has been processed.
X'3396'	Data transmit flow control blocked for pacing. **Explanation:** The connection over which this data flows is an ATM reserved bandwidth connection. More data has been requested to be sent than has been reserved. The data flow will be blocked for an interval of time to ensure data is not dropped by the ATM network. Data flow will be reopened when the interval of time passes.
X'3397'	Data transmit flow control blocked for remote **Explanation:** The connection over which this data flows is an ATM connection. The IBM Open Systems Adapter has reached a level of congestion and has requested that no more data be sent on this connection until the congestion is relieved. Data flow will be reopened by IBM Open Systems Adapter when the congestion condition has passed.
X'34nn'	n/a **Explanation:** Codes starting with X'34' are specific to the OSA-Express data path. These codes represent errors reported by the OSA-Express adapter relating to the read or write Storage Block Address List Entries (SBALEs).
X'3400'	Error reason unknown **Explanation:** The specific cause of the error cannot be determined.
X'3401'	Invalid buffer contents **Explanation:** The contents of the storage pointed to by the SBALE does not contain a valid OSA-Express header or IP header.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'3402'	Block crosses 4k boundary **Explanation:** The last byte of the storage represented by the SBALE is not contained in the same 4K storage frame as the first byte.
X'3403'	Invalid fragment type **Explanation:** The SBALE fragment type does not correlate with the fragment type of the previous SBALE.
X'3404'	Real address invalid **Explanation:** The SBALE storage address exceeds the size of central storage.
X'40nn'	n/a **Explanation:** Codes starting with X'40' are specific to the VTAM/IBM Open Systems Adapter IDX channel interface.
X'4001'	VTAM/IBM Open Systems Adapter function level mismatch **Explanation:** The IBM Open Systems Adapter returned this code indicating request failed due to function mismatch between VTAM and the IBM Open Systems Adapter; for example, incompatible versions of the two products. Contact system operator to determine cause of the incompatibility.
X'4002'	Incorrect or no header size specified **Explanation:** The IBM Open Systems Adapter returned this code indicating request failed during IDX exchange due to MPC specifying an improper header size. Contact VTAM operator to determine cause of the incorrect size.
X'4003'	Incorrect or no block size specified **Explanation:** The IBM Open Systems Adapter returned this code indicating request failed during IDX exchange due to MPC specifying an improper I/O buffer size. Contact VTAM operator to determine cause of the incorrect size.
X'4004'	Channel path read write polarity mismatch **Explanation:** The IBM Open Systems Adapter returned this code indicating request failed during IDX exchange due to incorrect channel path polarity; for example, read defined as write or write defined as read. The paths were defined incorrectly in either the TRL entry for the device or during IBM Open Systems Adapter configuration. Contact VTAM operator to determine cause of the incorrect size.
X'4005'	VTAM name mismatch **Explanation:** The IBM Open Systems Adapter returned this code indicating request failed during IDX exchange because the same VTAM name was not received over both channel paths. This indicates a condition where two different VTAM instances are configured such that one is trying to use the Read path, the other the Write. Contact VTAM operator to determine correct definition of channel paths.
X'4010'	Channel path pair quiesced **Explanation:** The IBM Open Systems Adapter returned this code indicating that channel paths will be halted due to the failure of some internal IBM Open Systems Adapter process. Contact system operator to determine reason for the IBM Open System Adapter's action.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'4011'	Incorrect data message size **Explanation:** The IBM Open Systems Adapter returned this code indicating an incorrect message size, normally too large. Channel operation is quiesced and the channel path to the IBM Open Systems Adapter becomes inoperative. Contact VTAM operator or system operator to determine correct maximum message size.
X'4080'	Normal termination **Explanation:** MPC uses this code to inform the IBM Open Systems Adapter that normal channel termination is required. It is not normally exposed to the ULP but might appear in the IBM Open Systems Adapter tracing facilities.
X'4081'	VTAM/IBM Open Systems Adapter level mismatch **Explanation:** MPC returned this code indicating initialization request failed due to function mismatch between VTAM and the IBM Open Systems Adapter; for example, incompatible versions of the two products. Contact VTAM operator or system operator to determine cause of the incompatibility.
X'4082'	Channel path read/write polarity error **Explanation:** MPC returned this code indicating initialization request failed due to the IBM Open Systems Adapter specifying an incorrect read or write channel address; the read channel address must be an "even" address and the associated write channel address must be the read address + 1.
X'4083'	Incorrect or no header size specified **Explanation:** MPC returned this code indicating initialization request failed due to the IBM Open Systems Adapter specifying an incorrect header segment size. Contact VTAM operator or system operator to determine cause of the incorrect size.
X'4084'	Incorrect or no buffer size **Explanation:** MPC returned this code indicating initialization request failed due to the IBM Open Systems Adapter specifying an incorrect I/O buffer size. Contact VTAM operator or system operator to determine cause of the I/O buffer size.
X'4085'	Data path failure **Explanation:** MPC returned this code indicating the channel paths to the IBM Open Systems Adapter are now inoperative due to a failure of the data path. Note, this is not a channel failure; it is the failure of a software component that processes data. Failure is normally due to an incorrect data primitive or the occurrence of a VTAM-detected processing error. Contact VTAM operator to perform problem diagnosis.
X'4086'	System failure **Explanation:** MPC returned this code indicating the failure of a process has caused an ABEND within MPC processing components. Failure might be due to an MPC software problem or an underlying system failure. Contact VTAM operator to perform problem diagnosis.
X'4087'	Channel path failure **Explanation:** MPC returned this code indicating the failure of the channel path between itself and the IBM Open Systems Adapter. Failure has been recorded as a long OBR record in the system log. Contact VTAM operator or the system operator to determine cause of failure.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'4088'	Token failure **Explanation:** MPC uses this code to indicate that the IBM Open Systems Adapter has returned inconsistent token values over the two channel paths. The tokens returned must contain identical bit strings. Contact the system operator to determine cause of inconsistency.
X'4089'	State mismatch **Explanation:** MPC uses this code to indicate that an inconsistency in processing states exists between MPC and the IBM Open Systems Adapter. Contact the VTAM operator to determine cause of inconsistency.
X'408A'	Event Notification Facility offline signal **Explanation:** MPC uses this code to indicate that an Event Notification Signal (ENF) has been received indicating the channel paths have been varied offline. Contact the system operator to determine reason the paths were put offline.
X'408B'	No storage for I/O buffer **Explanation:** MPC uses this code to indicate that storage was not available for it to build the required channel I/O buffers for the data and header segments. System storage might be constrained due to competing requests for storage. Contact the VTAM operator to determine VTAM's current storage usage and the system operator to determine cause of storage scarcity.
X'408C'	Incorrect IBM Open Systems Adapter name **Explanation:** The name used to activate the IBM Open Systems Adapter does not match the defined value. Check your definitions.
X'408D'	Channel control failure **Explanation:** MPC uses this code to indicate a failure in its channel control (CC) component. The failure might have been caused by a software failure in the CC component or an underlying system failure. Contact the VTAM operator to determine failure cause. If a system failure, notify the system operator.
X'408E'	Signaling plane failure **Explanation:** MPC uses this code to indicate a failure in the signaling plane. Contact the VTAM operator to determine failure cause. If a system failure, notify the system operator.
X'50nn'	Shared Memory Communications over Remote Direct Memory Access (SMC-R) failures **Explanation:** Codes starting with X'50' are specific to SMC-R operation failures. Use the specific return code to help identify the problem.
X'5001'	Peripheral Component Interconnect Express (PCIe) function ID (PFID) is not valid **Explanation:** The PFID value that is specified on the activation attempt contained characters that are not valid or that did not match the PFID of any active 10GbE RoCE Express interface.
X'5002'	The buffer size of the outbound buffer is not valid **Explanation:** The buffer size that is specified for a buffer to be used for outbound RDMA operations was too large or represented only a partial buffer.
X'5003'	The buffer size of the inbound buffer is not valid **Explanation:** The buffer size that is specified for a buffer to be used for inbound RDMA operations was too large or represented only a partial buffer.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5004'	The outbound RDMA buffer could not be registered **Explanation:** The buffer to be used for outbound RDMA operations could not be registered with the 10GbE RoCE Express interface because the buffer descriptor on the primitive request did not contain the correct information.
X'5005'	The inbound RDMA buffer could not be registered **Explanation:** The buffer to be used for inbound RDMA operations could not be registered with the 10GbE RoCE Express interface because the buffer descriptor on the primitive request did not contain the correct information.
X'5006'	Incorrect primitive **Explanation:** The value that is specified in the primitive code parameter of the control information field is not correct.
X'5008'	Maximum users exceeded **Explanation:** The activation request attempted for this adapter exceeds the allowable number of adapter users.
X'5009'	Internal state error **Explanation:** The primitive request is received in an unexpected adapter state.
X'500A'	Virtual LAN (VLAN) identifier is not valid **Explanation:** The value that is specified for the VLAN identifier on the activation request exceeds the maximum value allowed.
X'500B'	Incorrect SMC-R link activation message **Explanation:** The SMC-R link activation message that is received from the SMC-R peer contained no data or the data specified was incorrect.
X'500C'	Queue pair (QP) activation timed out **Explanation:** The attempt to activate a QP as part of SMC-R link establishment did not complete within an acceptable amount of time.
X'500D'	Internal abend **Explanation:** VTAM returns this code to indicate that the failure of a process caused an abnormal end of task (abend) within SMC-R processing components. A software problem or an underlying system failure might be the cause. Contact the VTAM operator to perform problem diagnosis.
X'500E'	Unable to schedule TCP/IP during interrupt processing **Explanation:** During a normal interrupt completion event, VTAM was unable to schedule the TCP/IP stack to process inbound data.
X'500F'	SMC-R VLAN disabled **Explanation:** The TCP/IP stack requested VTAM to disable a specific VLAN. As a result, all QPs that are associated with this VLAN are stopped.
X'5010'	RDMA over Converged Ethernet (RoCE) token is not valid **Explanation:** The value that is specified for the RoCE token on the primitive was 0 or did not match any currently assigned tokens.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5011'	VLAN token is not valid **Explanation:** The value that is specified for the VLAN token on the primitive did not match any currently assigned tokens.
X'5012'	QP token is not valid **Explanation:** The value that is specified for the QP token on the primitive was 0 or did not match any currently assigned tokens.
X'5013'	SMC-R link activation failure **Explanation:** VTAM could not successfully send the appropriate link activation message to the peer, preventing the SMC-R link from being activated.
X'5014'	Internal stall error detected **Explanation:** The SMC-R components determined that no outbound RDMA operations completed within an acceptable period. INOP processing is triggered for the 10GbE RoCE Express interface.
X'5015'	Internal poll error detected **Explanation:** An attempt by the SMC-R components to poll the 10GbE RoCE Express interface for information about outbound RDMA operations failed unexpectedly. INOP processing is triggered for the 10GbE RoCE Express interface.
X'5016'	Outbound RDMA operations cannot be queued **Explanation:** The SMC-R components determined that pending outbound RDMA operations must be queued because of 10GbE RoCE Express interface conditions, but this primitive indicated that it cannot be queued. The primitive is not queued.
X'5017'	Internal failure during 10GbE RoCE Express interface cleanup **Explanation:** The SMC-R components could not perform a final poll of the 10GbE RoCE Express interface for information about outbound RDMA operations before deactivating the 10GbE RoCE Express interface.
X'5018'	Could not schedule stack to process RDMA data **Explanation:** The SMC-R components could not schedule a TCP/IP process to receive RDMA data.
X'5019'	Queue pair (QP) activation timeout threshold exceeded **Explanation:** The SMC-R components detected repeated failures when activating a QP for an individual 10GbE RoCE Express interface. INOP processing is triggered for the interface.
X'5020'	A CSDUMP was taken with a defined RNICTRLE that matched this 10GbE RoCE Express interface **Explanation:** A CSDUMP operation, with the RNICTRLE operand specified, requested that diagnostic data be gathered for a 10GbE RoCE Express interface. The process of collecting this data rendered the 10GbE RoCE Express feature inoperative for all users.
X'5021'	10GbE RoCE Express interface deactivated because a hardware diagnostic dump was taken **Explanation:** A 10GbE RoCE Express interface was deactivated for one the following reasons: • An INOPDUMP was taken for the 10GbE RoCE Express interface. • A CSDUMP was taken and a diagnostic dump was requested by using the RNICTRLE parameter. **Note:** The gathering of diagnostic data causes an inoperative condition for all users.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5022'	10GbE RoCE Express interface deactivated because 10GbE RoCE Express internal error was detected **Explanation:** A 10GbE RoCE Express interface was deactivated because the interface reported an internal error. To recover from the internal error, VTAM resets the 10GbE RoCE Express interface and the 10GbE RoCE Express interface is temporarily unavailable for all users.
X'51nn'	10GbE RoCE Express device driver failure **Explanation:** In response to specific RoCE verb invocation failures, the 10GbE RoCE Express device driver sets the codes that start with X'51'. These codes are internally generated software codes that identify failures to communicate correctly with PCIe services or with the hardware. • For PCIe service failures, the 10GbE RoCE Express device driver issues message IST2390I or IST2391I to report these failures. In these cases, the *nn* portion of the error code represents the return code that was recorded for the specific PCIe service failure. • For all other failures, the *nn* portion of the error is an internally generated value to uniquely identify the failure.
X'5113'	PFID is not defined **Explanation:** The 10GbE RoCE Express device driver attempted to activate a 10GbE RoCE Express interface, but the PFIDs value is not defined for this LPAR. The 10GbE RoCE Express device driver issues message IST2392I to report this failure.
X'5115'	PFID is not online **Explanation:** The 10GbE RoCE Express device driver attempted to activate a 10GbE RoCE Express interface, but the PFID value is not configured online. The 10GbE RoCE Express device driver issues message IST2393I to report this failure.
X'5116'	Host channel adapter (HCA) configuration register (HCR) command operation timeout **Explanation:** The 10GbE RoCE Express device driver issued an HCR command to the RoCE hardware, but the hardware did not complete the operation within the internally specified timeout threshold. The 10GbE RoCE Express device driver initiates INOP processing to recover from this error.
X'5117'	PCIe load operation failure **Explanation:** During the processing of an HCR operation, the 10GbE RoCE Express device driver received an error in response to a PCIe load operation. The 10GbE RoCE Express device driver might initiate INOP processing to recover from this error.
X'5118'	PCIe store operation failure **Explanation:** During the processing of an HCR operation, the 10GbE RoCE Express device driver received an error in response to a PCIe store operation. The 10GbE RoCE Express device driver might initiate INOP processing to recover from this error.
X'5121'	HCR command operation failure **Explanation:** The 10GbE RoCE Express device driver issued an HCR command to the RoCE hardware, but the hardware rejected the operation with a specific status code. The specific HCR operation failed.
X'5131'	PCIe connect service call failure **Explanation:** The 10GbE RoCE Express device driver received an error in response to a PCIe connect service call (IQP4CON) during the activation of a 10GbE RoCE Express interface. The 10GbE RoCE Express device driver issues message IST2391I to report this failure.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5132'	PCIe open service call failure **Explanation:** The 10GbE RoCE Express device driver received an error in response to a PCIe open service call (IQP4OPN) during the activation of a 10GbE RoCE Express interface. The 10GbE RoCE Express device driver issues message IST2391I to report this failure.
X'5138'	PCIe deregister service call failure **Explanation:** The 10GbE RoCE Express device driver received an error in response to a PCIe deregister service call (IQP4DMR) in one of the following situations: • When a 10GbE RoCE Express interface is deactivated. • When the TCP/IP stack contracts a storage pool and attempts to deregister specific memory regions. The 10GbE RoCE Express device driver issues message IST2391I to report this failure.
X'513B'	Software reset failure **Explanation:** While the 10GbE RoCE Express device was initialized, the 10GbE RoCE Express device driver received an error during a software reset of the 10GbE RoCE Express feature. This call is issued during the activation of a 10GbE RoCE Express interface. The 10GbE RoCE Express interface does not activate.
X'5140'	PCIe close service call failure **Explanation:** The 10GbE RoCE Express device driver received an error in response to a PCIe close service call (IQP4CLO) during the deactivation of a 10GbE RoCE Express interface. The 10GbE RoCE Express device driver issues message IST2391I to report this failure.
X'5141'	PCIe deallocation service call failure **Explanation:** The 10GbE RoCE Express device driver received an error in response to a PCIe deallocation service call (IQP4DEA) during the deactivation of a 10GbE RoCE Express interface. The 10GbE RoCE Express device driver issues message IST2391I to report this failure.
X'5144'	PCIe allocation service call failure **Explanation:** The 10GbE RoCE Express device driver received an error in response to a PCIe allocation service call (IQP4ALL) during the activation of a 10GbE RoCE Express interface. The 10GbE RoCE device driver issues message IST2391I to report this failure.
X'514A'	No physical network ID detected **Explanation:** The 10GbE RoCE Express device driver issued a PCIe service call (IQP4GDI) to learn information about a 10GbE RoCE Express interface. The 10GbE RoCE Express device driver detected that no physical network ID (PNetID) was configured for this PFID. A 10GbE RoCE Express interface without a configured PNetID cannot be used for SMC-R communications. The 10GbE RoCE Express device driver issues message IST2391I to report this failure.
X'5150'	PCIe service processor call failure **Explanation:** The 10GbE RoCE Express device driver received an error in response to a PCIe service processor call (IQP4SPC) to collect diagnostic hardware information during the INOPDUMP or the CSDUMP processing. The 10GbE RoCE device driver issues message IST2391I to report this failure.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5151'	Incorrect operating environment detected for the IBM 10GbE RoCE Express feature **Explanation:** A 10GbE RoCE Express feature was configured in the hardware configuration definition (HCD) to run in a dedicated RoCE environment, but z/OS Communications Server expected the feature to run in a shared RoCE environment. Another possible situation is that a 10GbE RoCE Express feature was configured to run in a shared RoCE environment, but z/OS Communications Server expected the feature to run in a dedicated RoCE environment. The first 10GbE RoCE Express feature to be activated determines the operating environment for all subsequent features.
X'52nn'	TCP/IP SMC-R component failures during SMC-R processing **Explanation:** Codes that start with X'52' are specific to failures that are encountered within the TCP/IP SMC-R components during SMC-R processing. These errors cause the TCP connection to not use the SMC-R protocols.
X'52E0'	SMC-R link failure, no failover processing **Explanation:** The TCP/IP stack detected that an SMC-R link failed and no alternative SMC-R link was available.
X'52E1'	SMC-R link failure, local and remote partners are out of synch **Explanation:** The TCP/IP stack attempted to establish an initial SMC-R link to the remote partner, but the partner detects that an SMC-R link exists between the two endpoints.
X'52F0'	SMC-R link failure, failover processing **Explanation:** The TCP/IP stack detected that an SMC-R link failed. The TCP/IP stack switched the TCP connections that were using the failing SMC-R link to an alternative link within the SMC-R link group.
X'52F1'	SMC-R link failure, loss of path detected **Explanation:** The TCP/IP stack was notified that the RDMA path for an SMC-R link failed.
X'52F2'	SMC-R link failure, protocol violation **Explanation:** The TCP/IP stack detected that an SMC-R link failed because of a violation of the Link Layer Control (LLC) protocol that is used to manage the link.
X'52F3'	SMC-R link failure, RDMA write operation failed **Explanation:** The TCP/IP stack detected that an attempt to write RDMA data over an SMC-R link failed.
X'52F4'	SMC-R link failure, remote buffer confirmation failed **Explanation:** The TCP/IP stack detected that the remote partner did not confirm that an SMC-R link used a remote buffer. The link was stopped and, if possible, the TCP connections that were using the stopped link were switched to an alternative link in the link group.
X'52F5'	SMC-R link failure, delete buffer failed **Explanation:** The TCP/IP stack detected that the remote partner did not acknowledge that a buffer was no longer available for an SMC-R link to use. The link was stopped and, if possible, the TCP connections that were using the stopped link were switched to an alternative link in the link group.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'52F6'	SMC-R link failure, link deletion timed out **Explanation:** The TCP/IP stack attempted to delete an SMC-R link from a link group, but the remote partner did not acknowledge the request. The link was stopped and, if possible, the TCP connections that were using the stopped link were switched to an alternative link in the link group.
X'52F7'	SMC-R link failure, link test timed out **Explanation:** The TCP/IP stack tested the status of an SMC-R link, but the remote partner did not respond to the test request. The SMC-R link was assumed to be inactive and, if possible, the TCP connections that were using the stopped link were switched to an alternative link in the link group.
X'52F8'	SMC-R link failure, link addition timed out **Explanation:** The TCP/IP stack attempted to add an SMC-R link to a link group, but the remote partner did not acknowledge the request. The link was stopped and, if possible, the TCP connections that were using the stopped link were switched to an alternative link in the link group.
X'53nn'	TCP/IP stack failures during SMC-R processing **Explanation:** Codes that start with X'53' are specific to failures that the TCP/IP stack encountered during SMC-R processing. These errors cause the TCP connection to not use the SMC-R protocols.
X'54nn'	10GbE RoCE Express interrupt handler errors **Explanation:** Codes that start with X'54' are specific to failures that the 10GbE RoCE Express interrupt handlers encountered. The 10GbE RoCE Express interrupt handlers are associated with a 10GbE RoCE Express interface. These failures cause VTAM to initiate INOP processing of the 10GbE RoCE Express interface. For these failures, the *nn* portion of the error code represents the 1-byte event code that the 10GbE RoCE Express interface generates.
X'5409'	Port state event **Explanation:** The disabled interrupt exit was driven by PCIe services to notify the 10GbE RoCE Express device driver that the state of the 10GbE RoCE Express port is inactive. The 10GbE RoCE Express device driver initiates INOP processing for all TCP/IP stacks with active connections to this 10GbE RoCE Express interface.
X'54F0'	Allocation error exit **Explanation:** PCIe services drove the 10GbE RoCE Express allocation error exit to inform the 10GbE RoCE Express device driver of a PCIe error event. The 10GbE RoCE Express device driver initiates INOP processing for all TCP/IP stacks with active connections to this 10GbE RoCE Express interface.
X'54F1'	Open error exit **Explanation:** PCIe services requested the 10GbE RoCE Express open error exit to inform the TCP/IP stack that the PFID was deallocated. This code can be issued for one of the following reasons: • The 10GbE RoCE Express device driver detected an error that caused the Force Close processing to take down the 10GbE RoCE Express interface. • PCIe services detected a condition that required the deallocation of a PFID that VTAM allocated. In either case, the 10GbE RoCE Express device driver initiates INOP processing for the reported TCP/IP stack.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'54F2'	Event Queue (EQ) Doorbell error **Explanation:** The 10GbE RoCE Express device driver did a PCIe store operation to notify the 10GbE RoCE Express interface that the driver finished processing event queue elements. The store operation completed with an error. The 10GbE RoCE Express device driver initiates INOP processing for all TCP/IP stacks with active connections to the 10GbE RoCE Express interface.
X'55nn'	SMC-R link failure, RDMA write operation did not complete successfully **Explanation:** Codes that start with X'55' are specific to RDMA write-completion failures that are reported to the TCP/IP stack. These failures cause the TCP/IP stack to stop the SMC-R link that is associated with the failed RDMA write operation. If possible, the TCP/IP stack switches the TCP connections that are using the link to another link within the SMC-R link group. For these failures, the *nn* portion of the error code represents the 1-byte event code that the 10GbE RoCE Express interface generates to report the write completion failure.
X'56nn'	Shared Memory Communications - Direct Memory Access (SMC-D) failures **Explanation:** Codes that begin with X'56' are specific to SMC-D operation failures. Use the specific return code to identify the problem.
X'5601'	The buffer size of the outbound buffer is not valid **Explanation:** The size that was specified for a buffer to be used for outbound internal shared memory (ISM) operations was too large or represented only a partial buffer.
X'5602'	The ISM buffer could not be registered **Explanation:** The buffer to be used for ISM operations could not be registered because the buffer descriptor on the primitive request did not contain necessary information.
X'5603'	Incorrect primitive **Explanation:** The value that was specified in the primitive code parameter of the control information field is not correct.
X'5604'	Internal state error **Explanation:** The primitive request was received in an unexpected device state.
X'5605'	Virtual LAN (VLAN) identifier is not valid **Explanation:** The value that was specified for the VLAN identifier on the activation request exceeds the maximum allowed value.
X'5606'	Internal abend **Explanation:** VTAM returns this code to indicate that the failure of a process has caused an abnormal end of task (abend) within SMC-D processing components. The failure might be caused by a software problem or might be an underlying system failure. Contact the VTAM operator to diagnose the problem.
X'5607'	Internal failure during INOP processing **Explanation:** VTAM could not notify a user of the ISM device while processing an INOP condition.
X'5608'	Internal shared memory (ISM) token is not valid **Explanation:** The value that was specified for the ISM token on the primitive was 0 or did not match any currently assigned tokens.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5609'	VLAN token is not valid **Explanation:** The value that was specified for the VLAN token on the primitive was 0, exceeded the maximum allowed value, or did not match any currently assigned tokens.
X'560A'	SMC-D link token is not valid **Explanation:** The value that was specified for the SMC-D link on the primitive was 0 or did not match any currently assigned tokens.
X'560B'	No more buffers can be registered with the ISM device **Explanation:** The attempt to register a buffer for ISM operations failed because no index bits were available to represent the buffer. A maximum of 1920 buffers can be registered with an individual ISM device.
X'57nn'	Internal shared memory (ISM) function failure **Explanation:** Codes that begin with X'57' are specific to ISM verb invocation failures. For these failures, the 'nn' portion of the error code represents the return code that the ISM device generated in response to an ISM verb invocation.
X'5701'	PCIe Search (IQP4SRC) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe search service call (IQP4SRC) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5702'	No ISM PFIDs are defined for physical network ID (PNetID) **Explanation:** The ISM device driver issued a PCIe search service call (IQP4SRC) to detect all defined ISM PFIDs for the PNetID that is associated with the QDIO or iQDIO interface that the TCP/IP stack activated. The ISM device driver detected that no ISM PFIDs were defined for this specific PNetID. Therefore, the TCP/IP stack cannot use SMC-D communications for this PNetID. The ISM device driver issues message IST2422I to report this failure.
X'5703'	No ISM PFIDs are available for PNetID **Explanation:** The ISM device driver issued a PCIe search service call (IQP4SRC) to detect all defined ISM PFIDs for the PNetID that is associated with the QDIO or iQDIO interface that the TCP/IP stack activated. The ISM device driver detected that ISM PFIDs are defined for this PNetID, but none of the PFIDs are currently available. Therefore, the TCP/IP stack cannot use SMC-D communications for this PNetID. The ISM device driver issues message IST2423I to report this failure.
X'5704'	PCIe Get PFID Information (IQP4GPI) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe Get PFID Information service call (IQP4GPI) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5705'	PCIe Get Device Information (IQP4GDI) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe Get Device Information service call (IQP4GDI) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5706'	PCIe Register Memory Region (IQP4RMR) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe Register Memory Region service call (IQP4RMR). The ISM device driver issues message IST2391I to report this failure.

Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5707'	HVCommon storage allocation failure **Explanation:** The ISM device driver received an error in response to an IARV64 macro invocation to obtain high virtual common storage during the activation of an ISM interface.
X'5708'	Partner not reachable via SMC-D **Explanation:** The partner host supports SMC-D, but the partner is not reachable via SMC-D. For example, the partner host might be located on a different CEC, the partner host might not have SMC-D enabled for the same PNetID, or the defined VLANs for SMC-D are not consistent across the hosts.
X'5713'	PFID is not defined **Explanation:** The ISM device driver attempted to activate an ISM interface, but the PFID value that is detected through the PCIe search (IQP4SRC) service is not defined for this LPAR. The ISM device driver issues message IST2392I to report this failure.
X'5715'	PFID is not online **Explanation:** The ISM device driver attempted to activate an ISM interface, but the PFID value is not configured online. The ISM device driver issues message IST2393I to report this failure.
X'5717'	PCIe load operation failure **Explanation:** During the processing of an ICR operation, the ISM device driver received an error in response to a PCIe load operation. The ISM device driver might initiate INOP processing to recover from this error.
X'5718'	PCIe store operation failure **Explanation:** During the processing of an ICR operation, the ISM device driver received an error in response to a PCIe store operation. The ISM device driver might initiate INOP processing to recover from this error.
X'5721'	ICR command operation failure **Explanation:** The ISM device driver issued an ICR command to the ISM firmware, but the firmware rejected the operation with a specific command result. The specific ICR operation failed.
X'5731'	PCIe Connect (IQP4CON) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe connect service call (IQP4CON) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5732'	PCIe Open (IQP4OPN) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe open service call (IQP4OPN) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5738'	PCIe Deregister Memory Region (IQP4DMR) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe deregister service call (IQP4DMR) in one of the following situations: • When an ISM interface is deactivated. • When the TCP/IP stack contracts a direct memory buffer (DMB) storage pool and attempts to deregister specific memory regions. The ISM device driver issues message IST2391I to report this failure.

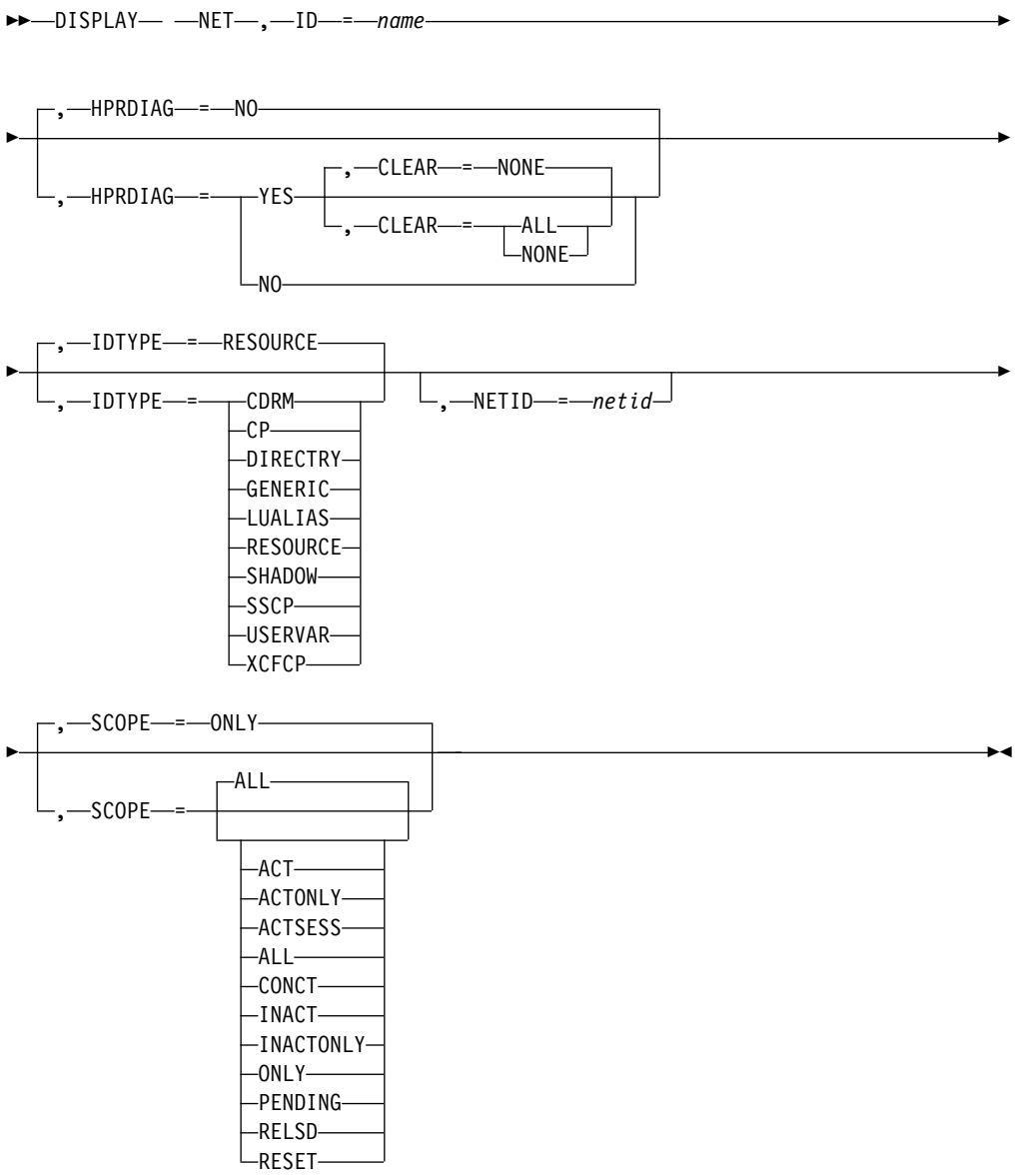
Table 17. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5740'	PCIe Close (IQP4CLO) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe Close service call (IQP4CLO) during the deactivation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5741'	PCIe Deallocation (IQP4DEA) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe deallocation service call (IQP4DEA) during the deactivation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5744'	PCIe Allocation (IQP4ALL) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe allocation service call (IQP4ALL) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5747'	Maximum number of registered direct memory buffers (DMBs) is reached **Explanation:** The TCP/IP stack attempted to expand the DMB storage pool by registering additional memory regions. The ISM device driver detected that it reached the maximum number of DMBs, which is allowed to register with ISM firmware. The DMB storage expansion request is failed.
X'5749'	Duplicate ICR operation **Explanation:** During the processing of an ICR operation, the ISM device driver received an error from the ISM firmware that the requested operation is a duplicate operation. The requested ISM operation was not performed.
X'574A'	Required hardware is not available **Explanation:** The ISM device driver detected that ISM processing cannot be performed because the necessary hardware is not available. The ISM device driver issues message IST2420I to report this failure.
X'574B'	PCIe Query System Characteristics (IQP4QSC) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe Query System Characteristics service call (IQP4QSC) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'58nn'	TCP/IP SMC-D componentry failures during SMC-D processing **Explanation:** Codes that begin with X'58' are specific to failures that are encountered within the TCP/IP SMC-D components during SMC-D processing. These errors cause the TCP connection to not use the SMC-D protocols.
X'59nn'	Internal shared memory (ISM) device interrupt handler errors **Explanation:** Codes that begin with X'59' are specific to failures that are encountered by the Disabled Interrupt Handler that is associated with an ISM device. These failures cause VTAM to initiate INOP processing of the ISM device. For these failures, the 'nn' portion of the error code represents the 1-byte event code that the ISM device generates.

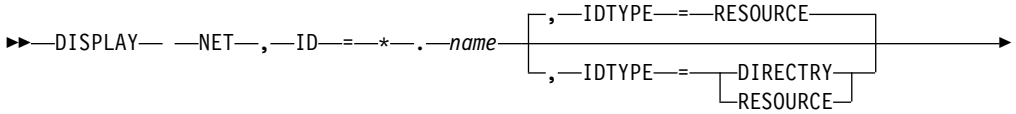
Chapter 8. SNA Operation

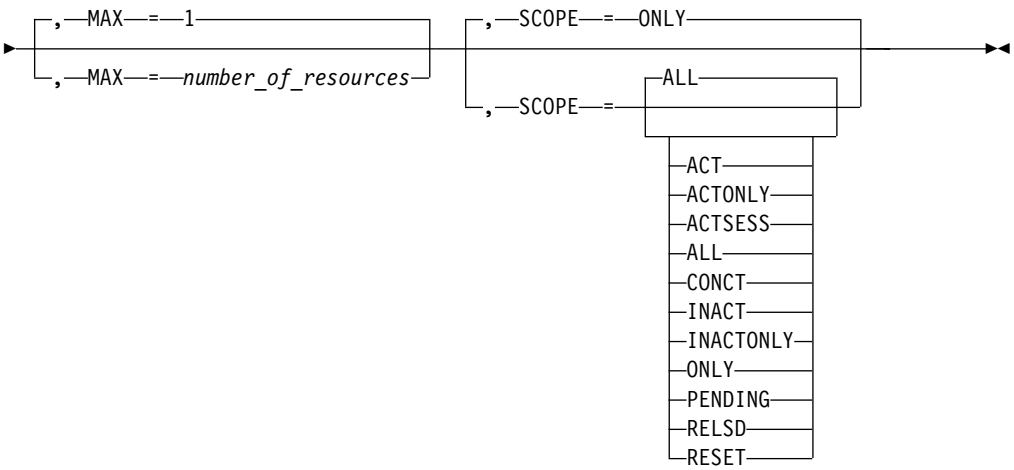
DISPLAY ID command

Display a resource:

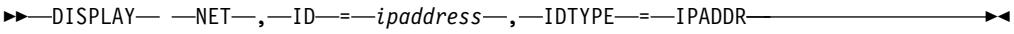


Display a resource name in any network:





Display a resource name using an IP address:



Abbreviations

Operand	Abbreviation
DISPLAY	D
HPRDIAG=YES	HPRDIAG or HPRDIAG=Y
SCOPE=ACT	ACT or A
SCOPE=ACTONLY	ACTONLY
SCOPE=ACTSESS	ACTSESS
SCOPE=ALL	EVERY or E
SCOPE=CONCT	CONCT
SCOPE=INACT	INACT or I
SCOPE=INACTONLY	INACTONL
SCOPE=ONLY	NONE or N
SCOPE=PENDING	PEND
SCOPE=RELSD	RELSD
SCOPE=RESET	RESET

When using an abbreviation in place of an operand, code the abbreviation exactly as shown in the table. For example, when coding the abbreviation for SCOPE=ALL, code only EVERY or E. Do not code SCOPE=E.

Purpose

The DISPLAY ID command provides information about a particular major node, minor node, or directory entry. Additional information can be displayed about the subordinate resources of the node.

Note: This command applies only to active major nodes and minor nodes within active major nodes.

Inactive subarea nodes (for example, NCP major nodes) that have been contacted by VTAM as a result of the activation of a cross-subarea link station can be displayed, if the name of the given subarea node is known to VTAM. Both the NCP being displayed and the NCP containing the link station must be an NCP V1R3 or later release level. In all other cases, inactive major nodes and their minor nodes are not known to VTAM and are therefore not displayed.

When the operator specifies:

- A switched line, the display indicates whether the line is dial-in, dial-out, or both dial-in and dial-out. For a dial-in line, the answer mode is indicated.
- An application program minor node or LU name, the associated z/OS UNIX System Services , interpret, and logon-mode table names and the default logon-mode entry are displayed.

  Note: Specifying ISTNOP, the name of the application program that represents the network operator, also displays the names of the message-flooding prevention table and the session awareness (SAW) data filter table.
- An NCP or host physical unit name, the following information is displayed:
  - The name and status of the associated dynamic path update members
  - The load module name of the NCP that was loaded (if different from the NCP PU name)
  - An indication of whether a nondisruptive load (MODIFY LOAD) is currently in progress
  - An indication of whether an NCP, MOSS, or CSP dump transfer (MODIFY DUMP) is currently in progress.
- The name of an FRSESET definition statement, an FRSESET display is issued. The display includes a message that shows how the FRSESET was defined, statically or dynamically. (Statically means that it was included in the NCP generation.)
- An application program minor node, the compression-level values are displayed.
- An application program, LU, or cross-domain resource name, the security data for data encryption and message authentication are displayed.

Operands

CLEAR
Specifies whether to clear diagnostic counters for the RTP pipe.

CLEAR=ALL
The diagnostic counters of the specified RTP pipe are cleared.

CLEAR=NONE
The diagnostic counters are not cleared.

The HPRDIAG=YES operand is required when you specify the CLEAR operand. The resource identified by the ID operand must be an RTP physical unit in this host.

HPRDIAG
Specifies whether additional HPR diagnostic information is to be displayed for the Rapid Transport Protocol (RTP) physical unit.

HPRDIAG=YES
Specifies that additional HPR diagnostic information is to be displayed for the Rapid Transport Protocol (RTP) physical unit.

The resource identified by the ID operand must be an RTP physical unit in this host.

HPRDIAG=NO
Specifies that additional HPR diagnostic information is not to be displayed for the Rapid Transport Protocol (RTP) physical unit. If specified, the resource identified by the ID operand must be an RTP physical unit in this host.

ID=name
Specifies the name of a major node, minor node, USERVAR, generic resource name, LUALIAS, or resource in the directory database.

The name can be a network-qualified name. Regardless of whether you specify a network-qualified name on the ID operand, the resource name in the display output is network-qualified only for application programs, SSCPs, CDRSCs, and LUs. The resource name in the display output is not network-qualified for any other type of resource.

For an APPN node, to display information about a dynamic XCF local SNA PU representing the connection to another VTAM, you can specify one of the following names:

- The name of the PU
- The CP name (or SSCP name) of the other VTAM with IDTYPE=XCFCP

For a pure subarea node, to display information about a dynamic XCF TRLE representing the connectivity to another VTAM node, you can specify one of the following names:

- The name of the TRLE
- The SSCP name (or CP name) of the other VTAM with IDTYPE=XCFCP

Note:

1. If the name is an NCP major node, the name used must be the name specified on the ID operand when the NCP was activated. If PUNAME was specified on the BUILD definition statement, then *name* is the PUNAME.
2. If the name is an application program in this domain, the ID operand can specify either the application program minor node name or the name under which the application program opened its ACB.
3. For an application program minor node, you can specify the name of a conventionally defined application program, a model application program, or a dynamic application program built from a model application program definition. For a CDRSC minor node, you can specify the name of a conventionally defined CDRSC, a model CDRSC, a clone CDRSC built from a model CDRSC, or a dynamic CDRSC.

   If you are specifying a model resource (APPL or CDRSC), you can use wildcard characters in the name you specify. The use of wildcard characters on the ID operand of the DISPLAY ID command does not depend on the value of the DSPLYWLD start option. Unlike wildcard characters in other commands, the wildcard characters you specify on the ID operand of the DISPLAY ID command do not represent unspecified characters. They are interpreted as the actual characters, asterisk (*) and question mark (?).

   Therefore, if you specify DISPLAY ID=APPL*, VTAM displays information about the model resource (APPL or CDRSC) named APPL*, but it does not display information about any other application programs or CDRSCs

whose names begin with APPL, followed by zero to four valid characters in length. It also does not display detailed information about any clone resource (APPL or CDRSC) that was built from the model resource named APPL*.

In other words, using wildcard characters in the name that you specify on the ID operand of the DISPLAY ID command results in the display of at most one model application program or one model CDRSC. If you want to display information about all application programs or CDRSCs whose names match a pattern established by the placement of wildcard characters, use the DISPLAY RSCLIST command.

4. For a CDRM, you can specify a network-qualified name, but this does not remove the restriction that the non-network-qualified CDRM name must be unique across networks.
5. If the name is a non-network-qualified CDRSC, VTAM uses the network ID of the host from which the command is issued. If two or more CDRSCs exist with the same resource name, but different network identifiers, and DISPLAY ID=*non-network-qualified_name* is issued, then one of the following situations occurs:
   - Only one CDRSC is displayed. The displayed CDRSC is one of the following types:
     - The one that has been defined with VTAM's network identifier
     - The one that has been defined as cross-network, but specified with NQNMODE=NAME, either on its CDRSC definition or by the NQNMODE start option
   - None of the CDRSCs are displayed if they are all specified with NQNMODE=NQNAME, either on their CDRSC definitions or by the NQNMODE start option.
6. If you specify a non-network-qualified USERVAR name, VTAM uses the network ID of the host from which you issue the command.
7. You can specify an asterisk (*) as a wildcard character (or *NETWORK) as the network ID portion of a network-qualified name. The wildcard character (*) is useful for displaying a resource for which you do not know the network ID. The wildcard character (*) is also useful for displaying several resources with the same name that are found in multiple networks, if you also specify the MAX operand on the command.
8. If the name is a generic resource name, the output lists all the members known by that generic resource name.
9. If the name is a TN3270 client IP address in dotted decimal format (for example, ID=192.5.48.122) or in colon-hexadecimal format for IPv6 addresses and there is an associated z/OS Communications Server Telnet server APPL, CDRSC, or LU minor node resource name, it is displayed. The saving and displaying of the IP information for TN3270 clients is controlled by the IPINFO start option. See z/OS Communications Server: SNA Resource Definition Reference for more information about the IPINFO start option.
10. If the name is an RTP pipe, the number of fully active sessions is displayed in the IST1855I message.

Restriction: When you specify an IP address, **IDTYPE=IPADDR** is also required.

IDTYPE
Specifies the type of resource that the ID operand names. If several types of

resources share the same name, IDTYPE can be used to identify which resource the command acts on. IDTYPE differs from MAX in that IDTYPE displays several representations of the same resource, whereas MAX displays several different resources with the same name.

IDTYPE=CDRM
Displays information only about the SSCP (represented as a CDRM).

IDTYPE=CP
Displays information only about the host CP (represented as an application) or an adjacent CP (represented as a CDRSC).

IDTYPE=DIRECTRY
Displays information from the directory database for the specified resource. The DISPLAY ID command with IDTYPE=DIRECTRY is valid only when it is issued at a network node or an interchange node.

IDTYPE=GENERIC
Displays the names of application program network names that are also generic resources.

IDTYPE=IPADDR
Displays the IP address of the currently connected TN3270 client applications and LUs. The IP address accepts a fully qualified dotted decimal format for IPv4 type addresses, or colon-hexadecimal format for IPv6 type addresses.

Note: The saving and displaying of the IP information for TN3270 clients is controlled by the IPINFO start option. See z/OS Communications Server: SNA Resource Definition Reference for more information.

IDTYPE=LUALIAS
Displays information only about the CDRSC whose name is associated with the LUALIAS. If a network-qualified name is specified, VTAM does not search for an LUALIAS with that resource name. For more information about CDRSCs that are defined with an LUALIAS, see z/OS Communications Server: SNA Resource Definition Reference.

IDTYPE=RESOURCE
Displays information about the resource named on the ID operand. VTAM searches for the resource in the following order:

1. VTAM searches for an SSCP (CDRM), a host CP (application), or an adjacent CP (CDRSC) by the name specified on the ID operand and displays information for any or all these resources it finds. If the resource is found and it is not the host CP, and you are issuing this command at a network node or interchange node, the display includes information from the directory database.
2. If VTAM does not find an SSCP, a host CP, or an adjacent CP, it searches for a resource with the name specified on the ID operand and displays information for the resource, if it finds it. If the resource is a CDRSC, and you are issuing this command at a network node or interchange node, the display includes information from the directory database.
3. If VTAM does not find a resource by that name, it searches for a USERVAR with the name specified on the ID operand and displays information for the resource, if it finds it.
4. If VTAM does not find a USERVAR by that name, or a USERVAR is found but the resource defined as the value of the USERVAR is not

found, it searches for an LUALIAS with the name specified on the ID operand and displays information for the CDRSC, if it finds it.

5. If no resource is found with the name specified on the ID operand, and you are issuing this command at a network node or interchange node, VTAM displays information about the resource from the directory database, if it finds it.
6. If no resource is found and no entry exists in the directory database with the specified name, the command fails.

IDTYPE=SHADOW
Displays information only about a shadow resource, if it exists. Included in the information displayed is the real resource that caused the displayed resource to become a shadow resource.

For more information about shadow resources, see the z/OS Communications Server: SNA Network Implementation Guide

IDTYPE=SSCP
Displays information only about the SSCP (represented as a CDRM).

IDTYPE=USERVAR
Displays information only about the resource whose name is associated with the USERVAR.

IDTYPE=XCFCP
Displays information only about the dynamic XCF local SNA PU representing the connection to another VTAM in the XCF group, when the ID operand specifies the CP name of the other VTAM.

MAX=number_of_resources
Specifies the maximum number of resources to display when the resource name on the ID operand is specified as being in "any network". That is, the network ID portion of the network-qualified resource name is specified as * (or *NETWORK). For example, ID=*.a01n can be specified. MAX is valid only when the following conditions are both true:

1. An "any network" resource name is specified on the ID operand
2. IDTYPE=RESOURCE or IDTYPE=DIRECTRY is used

The value for MAX can be any integer from 1 to 200. The default is 1.

The resource name might exist in more networks than the number you specify on the MAX operand. However, VTAM searches only for the number of instances that you have specified. When that number is found, VTAM does not search any further. This saves processing time for the command and gives you control over the amount of display output generated by the command. If fewer resources are found than you have specified on MAX, VTAM displays only the resources that are found.

The display might show the same resource more than once if both subarea information and APPN directory information are available for a particular resource. The value specified for MAX does not consider this duplication of information for a particular resource, so you could specify a value such as MAX=3 and receive a display of up to six resources.

NETID=netid
Valid only for CDRSC major nodes and limits the scope of the display to CDRSCs within the indicated network and CDRSCs defined without a network identifier (not associated with any particular network). If you specify the NETID operand, but do not identify a specific network (that is, a value for

netid is not entered), all CDRSCs in the major node are displayed. CDRSCs are displayed in the order in which they were defined or added within the major node.

To display minor nodes and independent LUs, specify a network-qualified name on the ID operand, and do not use the NETID operand.

SCOPE
Specifies the wanted scope of the display.

Note: If you specify the SCOPE operand without specifying a value SCOPE=ALL is assumed.

The SCOPE operand is ignored for frame relay PUs or FRSESETs. Nor does SCOPE have any effect when you display resources in the directory database.

These values specify whether information is to be provided about the specified node's subordinate resources in addition to the information about the node itself. They are meaningful only for resources that have subordinate resources.

SCOPE=ACT
Specifies that, in addition to the resource specified on the ID operand, the name, and status of all its active, pending, and connectable subordinate resources, if any, are to be displayed. If this display is undesirably large, you can use SCOPE=ACTONLY or SCOPE=CONCT to further limit the display.

SCOPE=ACTONLY
Specifies that, in addition to the resource specified on the ID operand, the name, and status of all its active subordinate resources, if any, are to be displayed. The display does not include resources in pending or connectable states. If no resources are found in an active state, you can use SCOPE=ACT to broaden the scope of the display to active, connectable, and pending resources.

SCOPE=ACTSESS
Specifies that, in addition to the resource specified on the ID operand, the name of all its subordinate resources that are active with sessions, if any, are to be displayed.

SCOPE=ALL
Specifies that, in addition to the resource specified on the ID operand, the name, and status of all its subordinate resources, if any, are to be displayed (regardless of their status).

SCOPE=CONCT
Specifies that, in addition to the resource specified on the ID operand, the name, and status of all its subordinate resources in a CONCT (connectable) state, if any, are to be displayed. If no resources are found in a connectable state, you can use SCOPE=ACT to broaden the scope of the display to active, connectable, and pending resources.

SCOPE=INACT
Specifies that, in addition to the resource specified on the ID operand, the name, and status of all its inactive subordinate resources, if any, are to be displayed. If this display is undesirably large, you can use SCOPE=INACTONLY or SCOPE=RESET to further limit the display.

SCOPE=INACTONLY
Specifies that, in addition to the resource specified on the ID operand, the

name, and status of all its inactive subordinate resources, if any, are to be displayed. Resources in a RESET state are not included in the SCOPE=INACTONLY display.

SCOPE=ONLY
Tells VTAM not to display the name and status of any subordinate resources.

SCOPE=PENDING
Specifies that, in addition to the resource specified on the ID operand, the name, and status of all its pending subordinate resources, if any, are to be displayed. A pending state is a transient state to or from the fully active state.

SCOPE=RELSD
Specifies that the information is to be displayed about all PUs in a RELSD state within the specified major nodes.

SCOPE=RESET
Specifies that, in addition to the resource specified on the ID operand, the name, and status of all its subordinate resources in a RESET state, if any, are to be displayed.

Resulting display

The resources that are displayed depend on their relationship within the hierarchy that is specified on the ID operand. The following lists show what resources are displayed for each major node or minor node.

Note: Independent LUs that are defined under a PU do not always appear in this output. Only independent LUs that are currently using the PU as a boundary function for multiple concurrent sessions are displayed.

A DISPLAY ID command issued at an APPN node might show a resource name appearing in several networks even though the resource actually exists in only one network. This can happen if intermediate SSCPs are pre-V4R1 and they pass only the 8-character resource name. The real network ID is therefore lost and other network IDs might be subsequently assumed.

For a DISPLAY ID command with IDTYPE=RESOURCE or IDTYPE=DIRECTRY, if the resource type that is displayed is EN, the node might actually be a network node, end node, or SSCP. This is because in a mixed APPN and subarea network, CPs, and SSCPs that are found in or through a subarea network are represented in this host (the host where you are issuing this command) as end nodes which are served by the interchange node through which the resource was found.

Note: If model application program definitions are included in the display, any dynamic application programs built from those models that have been deactivated are not displayed. This is because dynamic application programs cannot exist in an inactive state. When a dynamic application program is deactivated and CLOSE macro processing is complete for the dynamic application program, the definition of the dynamic application program is deleted. The dynamic application program is no longer known by VTAM and will not appear in the output of any DISPLAY commands.

- Major nodes:
  - For ID=*ADJCP major node*, its subordinate nodes
  - For ID=*application program major node*, its subordinate applications:

        - Conventionally defined application programs
        - Model application programs
        - Dynamic application programs built from model application program definitions
      – For ID=*CDRM major node*, its subordinate CDRMs
      – For ID=*CDRSC major node*, its subordinate CDRSCs:
        - Conventionally defined CDRSCs
        - Model CDRSCs
        - Clone CDRSCs built from model CDRSC definitions
      – For ID=*channel-attachment major node*, its subordinate links
      – For ID=*external communications adapter (XCA) major node*, its subordinate links
      – For ID=*hostpu*, its subordinate cross-subarea links
      – For ID=*local non-SNA 3270 major node*, its subordinate logical units
      – For ID=*local_sna_major_node*:
        - Each PU providing local SNA connectivity and its subordinate logical units
        - Each PU providing APPN host-to-host connectivity
      – For ID=*lugroup major node*, its model LU groups, and their model LUs
      – For ID=*model major node*, its subordinate logical units and the physical units to which the logical units are subordinate
      – For ID=*NCP major node*, its subordinate links
      – For ID=*rapid transport protocol major node* (ISTRTPMN), its dynamic physical units
      – For ID=*switched major node*, its subordinate logical units and the physical units to which the logical units are subordinate
      – For ID=*transport resource list major node*, its subordinate transport resource list entries (TRLEs).
  - Minor nodes:
      – For ID=*conventionally defined application program* or ACB *name*:
        - For SCOPE=ACT, the established sessions with the application program
        - For SCOPE=INACT, the names of logical units waiting for sessions with the application program
        - For SCOPE=ALL, the information provided for both ACT and INACT, as described above
        - An indication if the application is a VCNS user
      – For ID=*model application program*
        - An indication that the application program is a model
        - A list of dynamic application programs that have been built from this model, or an indication that no dynamic application programs have been built from this model
        - An indication if the model application program definition specifies that any dynamic application programs built from the model are to be VCNS users
      – For ID=*dynamic application program*
        - An indication that the application program is a dynamic application program
        - The name of the model application program definition used to build the dynamic application program

- For SCOPE=ACT, the established sessions with the dynamic application program
- For SCOPE=ALL, the established sessions with the dynamic application program
- An indication if the dynamic application program is a VCNS user

– For ID=*CDRSC minor node* (conventionally defined and dynamic):
- For SCOPE=ACT, the established sessions with the cross-domain resource
- For SCOPE=INACT, the names of logical units waiting for sessions with the cross-domain resource
- For SCOPE=ALL, the information provided for both ACT and INACT, as described in the preceding information

– For ID=*model CDRSC minor node*:
- An indication that the CDRSC is a model
- An indication of the current value of the DELETE parameter of the model CDRSC
- For SCOPE=ONLY, an indication if no clone CDRSCs currently exist that were built from this model
- For other values of SCOPE, a list of clone CDRSCs that have been built from this model that meet the SCOPE criteria, or an indication if no clone CDRSCs currently exist that were built from this model that meet the SCOPE criteria

– For ID=*clone CDRSC minor node*:
- An indication that the CDRSC is a clone
- The name of the model CDRSC used to build the clone CDRSC
- An indication of the current value of the DELETE parameter from the model CDRSC used to build this clone CDRSC
- For SCOPE=ACT, the established sessions with the cross-domain resource
- For SCOPE=INACT, the names of logical units waiting for sessions with the cross-domain resource
- For SCOPE=ALL, the information provided for both ACT and INACT, as described previously

– For ID=*host* CDRM *name*, the host's network ID (where applicable), subarea and element addresses, and only the external CDRM session partner and session status for established sessions with the host CDRM

– For ID=*same-network external* CDRM *name*:
- HPR capability, if the same-network external CDRM is active
- For SCOPE=ACT, active cross-domain resources owned by the external CDRM
- For SCOPE=INACT, inactive cross-domain resources owned by the external CDRM
- For SCOPE=ALL, all active or inactive cross-domain resources owned by the external CDRM

– For ID=*cross-network external* CDRM *name*:
- For SCOPE=ACT, active cross-network resources owned by the external CDRM
- For SCOPE=INACT, inactive cross-network resources owned by the external CDRM
- For SCOPE=ALL, all active or inactive cross-network resources owned by the external CDRM

  - For ID=*line group*:
    - For SCOPE=ALL, lines and PUs
    - For SCOPE=ACT, all active lines and all active PUs
    - For SCOPE=INACT, all inactive lines, all inactive PUs, and all active lines that have inactive PUs
    - For SCOPE=ONLY, only line group
  - For ID=*link*:
    - Its subordinate link stations, or
    - Its subordinate physical units and dependent logical units
  - For ID=*physical_unit*:
    - Its subordinate logical units
    - For a PU providing APPN host-to-host connectivity, the name, status, and line control as specified by the TRLE operand on the PU definition statement
    - For a PU supported by a DLUR, the name of the DLUR and the switched major node that defines the PU
    - For a dynamic rapid transport protocol (RTP) PU, the data flow rate and the end-to-end route
    - For an HPR-capable PU in a type 2.1 node, the HPR capability.
  - For ID=*transport_resource_list_entry*:
    - Names of the Communications Server z/OS upper-layer protocols (ULPs) using this TRLE
    - For a dynamic TCP TRLE, an exclusively owned TRLE, or an internal shared memory (ISM) TRLE, only one message with a ULP ID is issued because only one ULP can use each of these TRLEs. For an OSA-Express adapter, one message with a ULP ID is issued for each datapath channel address that a ULP uses. For other TRLEs, more than one ULP ID message can be issued, depending on how many ULPs are using the TRLE.

      Rule: Only one message with a ULP ID is generated for a 10GbE RoCE Express feature that operates in a shared RoCE environment.
    - The ULP ID will be the jobname for TCP/IP ULPs, the SNA PU name for ANNC ULPs, and the XCA Major Node name for ATM or EE ULPs.
- Resources in the directory database:
  - The name of the resource
  - The entry type, such as dynamic
  - The resource type, such as network node
  - The owning CP
  - The network node server
  - For an LU resource:
    - The subarea number
    - The required locate message size to retrieve routing information
    - The locate message size used when this LU was last searched
- Generic resource names:
  - Member name
  - Owning CP name
  - Whether the resource is currently available to be selected during resolution. `NO` indicates that the generic resource is on an end node that does not have a

CP-CP session with its network node server, and is therefore not selectable. YES indicates that the resource is selectable. DEL indicates that the resource has deleted itself as a generic resource and is not selectable. If you need to fully delete the generic resource from VTAM and the generic resource coupling facility structure, the application's ACB must be closed and the MODIFY GR DELETE command must be issued at every host in the sysplex. See the z/OS Communications Server: SNA Network Implementation Guide for a full description of generic resource deletion procedures.

– APPC value

Examples

Displaying an adjacent CP major node:

```
d net,id=istadjcp,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = ISTADJCP, TYPE = ADJCP MAJOR NODE
IST486I STATUS= ACTIV     ,  DESIRED STATE= ACTIV
IST1100I ADJACENT CONTROL POINTS FROM MAJOR NODE ISTADJCP
IST1102I NODENAME          NODETYPE CONNECTIONS CP CONNECTIONS NATIVE
IST1103I NETB.VN1          VN       0           0              *NA*
IST2157I ALIASRCH = *NA
IST1103I NETA.VN1          VN       1           0              *NA*
IST2157I ALIASRCH = *NA
IST314I END
```

Displaying an application program major node, including model application programs and dynamic application programs built from those models:

```
d net,id=a01appls,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A01APPLS, TYPE = APPL SEGMENT
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST360I APPLICATIONS:
IST080I APPL01   CONCT      APPL0102 CONCT      A01MVSNO CONCT
IST080I APPL1    CONCT      APPLA*   CONCT      APPL2    CONCT
IST080I APPLQ?   CONCT      APPL3    CONCT      APPLQ1   ACTIV
IST314I END
```

Displaying a CDRM major node:

```
d net,id=cdrm1a,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = CDRM1A, TYPE = CDRM SEGMENT
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST477I CDRMS:
IST1546I CDRM     STATUS    SUBAREA ELEMENT NETID    SSCPID
IST1547I SSCP1A    ACTIV          1      1  NETA          1
IST1547I SSCPAA    NEVAC         10      1  NETA        N/A
IST1547I SSCP2A    NEVAC          2      1  NETA        N/A
IST1547I SSCPBA    NEVAC         11      1  NETA        N/A
IST1547I SSCPCA    NEVAC         12      1  NETA        N/A
IST1547I SSCP7B    ACTIV          5      1  NETB          7
IST1547I SSCP9C    ACTIV          8      3  NETC          9
IST1500I STATE TRACE = OFF
IST314I END
```

Displaying a CDRSC major node:

```
d net,id=istcdrdy,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = ISTCDRDY, TYPE = CDRSC SEGMENT
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST478I CDRSCS:
IST483I C25NVLUC ACTIV----Y, CDRM = ***NA***, NETID = NETA
```

```
IST483I B01NVLUC ACTIV----Y, CDRM = ***NA***, NETID = NETA
IST483I A81NVLUC ACTIV----Y, CDRM = ***NA***, NETID = NETA
IST483I A03D207F ACT/S----Y, CDRM = A01N    , NETID = NETA
IST483I A02NVLUC ACT/S----Y, CDRM = A01N    , NETID = NETA
IST483I ECHO02A  ACT/S----Y, CDRM = A01N    , NETID = NETA
IST483I A50NVLUC ACT/S----Y, CDRM = A01N    , NETID = NETA
IST483I A500N    ACT/S----Y, CDRM = A01N    , NETID = NETA
IST483I A02N     ACT/S----Y, CDRM = A01N    , NETID = NETA
IST314I END
```

Displaying a CDRSC major node for a specific network:

```
d net,id=a99cdrsc,netid=netc,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A99CDRSC, TYPE = CDRSC SEGMENT
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST478I CDRSCS:
IST483I CECH*    ACTIV     , CDRM = C01M    , NETID = NETC
IST483I CECHO01  ACTIV     , CDRM = C01M    , NETID = NETC
IST483I TPNSC01  ACTIV     , CDRM = C01M    , NETID = NETC
IST483I C01NVLUC ACTIV     , CDRM = C01M    , NETID = NETC
IST483I TSO11    ACTIV     , CDRM = ***NA***, NETID = NETC
IST483I ECHO11   ACTIV     , CDRM = C11M    , NETID = NETC
IST483I C11NVLUC ACTIV     , CDRM = C11M    , NETID = NETC
IST483I TSO255   ACTIV     , CDRM = ***NA***, NETID = NETC
IST483I ECHO255  ACTIV     , CDRM = C255M   , NETID = NETC
IST483I C255NLUC ACTIV     , CDRM = C255M   , NETID = NETC
IST314I END
```

Displaying a local SNA major node:

```
d net,id=a50lsna,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A50LSNA, TYPE = LCL SNA MAJ NODE
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST084I NETWORK NODES:
IST089I PUA      TYPE = PU_T2            , ACTIV      ,CUA=0770
IST089I LSNALU1  TYPE = LOGICAL UNIT     , ACTIV
IST089I LSNALU2  TYPE = LOGICAL UNIT     , ACTIV
IST089I LSNALU3  TYPE = LOGICAL UNIT     , ACTIV
IST089I LSNALU4  TYPE = LOGICAL UNIT     , ACTIV
IST314I END
```

Displaying a local SNA major node for each PU providing APPN host-to-host connectivity:

```
d net,id=lsna1a,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = LSNA1A, TYPE = LCL SNA MAJ NODE
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST084I NETWORK NODES:
IST1316I PU NAME = AHHCPU1   STATUS = NEVAC       TRLE = ML1A2A2
IST1316I PU NAME = AHHCPU2   STATUS = NEVAC       TRLE = ML1A2A3
IST1316I PU NAME = AHHCPU3   STATUS = NEVAC       TRLE = ML1A2A4
IST314I END
```

Displaying the dynamic XCF local SNA major node:

```
d net,id=istlsxcf,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = ISTLSXCF, TYPE = LCL SNA MAJ NODE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST084I NETWORK RESOURCES:
IST1316I PU NAME = ISTP0001  STATUS = ACTIV--LX-  TRLE = ISTT0001
IST1500I STATE TRACE = OFF
IST314I END
```

Displaying a transport resource list major node:

```
d net,id=trl1a,scope=all
 IST097I DISPLAY ACCEPTED
 IST075I NAME = TRL1A, TYPE = TRL MAJOR NODE
 IST1314I TRLE = TRLE1A    STATUS = NEVAC       CONTROL = MPC
 IST1314I TRLE = TRLE1B    STATUS = NEVAC       CONTROL = MPC
 IST1314I TRLE = TRLE1C    STATUS = NEVAC       CONTROL = MPC
 IST1314I TRLE = TRLE1D    STATUS = NEVAC       CONTROL = MPC
 IST314I END
```

Displaying an active TRL entry:

```
d net,id=trle1a
IST097I DISPLAY ACCEPTED
IST075I NAME = TRLE1A, TYPE = TRLE
IST486I STATUS= ACTIV----E, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = MPC , HPDT = NO
IST1954I TRL MAJOR NODE = TRL1
IST1715I MPCLEVEL = HPDT       MPCUSAGE = SHARE
IST1221I WRITE DEV = 0508 STATUS = RESET      STATE = ONLINE
IST1221I READ  DEV = 0408 STATUS = RESET      STATE = ONLINE
IST1500I STATE TRACE = OFF
IST314I END
```

Displaying a local non-SNA 3270 major node:

```
d net,id=a01local,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A01LOCAL, TYPE = LCL 3270 MAJ NODE
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST355I LOGICAL UNITS:
IST089I A01A741  TYPE = LOGICAL UNIT     , NEVAC      ,CUA=0741
IST089I A01A742  TYPE = LOGICAL UNIT     , NEVAC      ,CUA=0742
IST089I A01A743  TYPE = LOGICAL UNIT     , NEVAC      ,CUA=0743
IST089I A01A744  TYPE = LOGICAL UNIT     , NEVAC      ,CUA=0744
IST089I A01A745  TYPE = LOGICAL UNIT     , NEVAC      ,CUA=0745
IST089I A01A746  TYPE = LOGICAL UNIT     , NEVAC      ,CUA=0746
IST089I A01A747  TYPE = LOGICAL UNIT     , NEVAC      ,CUA=0747
IST089I A01A748  TYPE = LOGICAL UNIT     , NEVAC      ,CUA=0748
IST089I A01A721  TYPE = LOGICAL UNIT     , ACT/S      ,CUA=0721
IST089I A01A722  TYPE = LOGICAL UNIT     , ACTIV      ,CUA=0722
IST089I A01A723  TYPE = LOGICAL UNIT     , ACTIV      ,CUA=0723
IST089I A01A724  TYPE = LOGICAL UNIT     , ACTIV      ,CUA=0724
IST089I A01A725  TYPE = LOGICAL UNIT     , ACTIV      ,CUA=0725
IST089I A01A726  TYPE = LOGICAL UNIT     , NEVAC      ,CUA=0726
IST314I END
```

Displaying an NCP major node:

```
d net,id=a0462zc,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A0462ZC, TYPE = PU T4/5
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST247I LOAD/DUMP PROCEDURE STATUS = RESET
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST484I SUBAREA = 4
IST391I ADJ LINK STATION = 0017-S, LINE = 0017-L, NODE = ISTPUS
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST077I SIO = 50078 CUA = 0017
IST675I VR = 0, TP = 2
IST170I LINES:
IST080I A04B00   NEVAC      A04B01   NEVAC      A04B03   NEVAC
IST080I A04B32   NEVAC      A04B33   NEVAC      A04B35   NEVAC
IST080I A04VXX   NEVAC----T A04S02   NEVAC      A04S34   NEVAC
IST080I A04S04   NEVAC      A04S16   NEVAC      A04S20   NEVAC
```

```
IST080I A04S36   NEVAC      A04S48   NEVAC      A04S52   NEVAC
IST080I A04S128  NEVAC      A04S136  NEVAC      A04PT88  ACTIV
IST080I A04C00   NEVAC      A04C02   NEVAC
IST314I END
```

Displaying the host physical unit:

```
d net,id=istpus,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = ISTPUS, TYPE = PU T4/5
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST596I IRN TRACE = OFF
IST1656I VTAMTOPO = INCLUDE, NODE REPORTED - YES
IST484I SUBAREA = 1
IST925I DYNAMIC PATH DEFINITION PATH1A STATUS = ACTIV
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST170I LINES:
IST080I 091C-L   ACTIV----I
IST314I END
```

Displaying the rapid transport protocol (RTP) major node:

```
d net,id=istrtpmn,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = ISTRTPMN, TYPE = RTP MAJOR NODE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1486I   RTP NAME   STATE             DESTINATION CP     MNPS  TYPE
IST1487I   CNR00004   CONNECTED         NETA.SSCP2A        NO    LULU
IST1487I   CNR00003   CONNECTED         NETA.SSCP2A        NO    RSTP
IST1487I   CNR00002   CONNECTED         NETA.SSCP2A        NO    CPCP
IST1487I   CNR00001   CONNECTED         NETA.SSCP2A        NO    CPCP
IST314I END
```

Displaying a switched major node:

```
d net,id=a04smnc,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A04SMNC, TYPE = SW SNA MAJ NODE
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST084I NETWORK NODES:
IST089I A04P882  TYPE = PU_T2            , ACTIV--L--
IST089I A04P883  TYPE = PU_T2            , ACTIV--L--
IST089I A04D8831 TYPE = LOGICAL UNIT     , ACTIV
IST089I A04D8832 TYPE = LOGICAL UNIT     , ACTIV
IST089I A04D8833 TYPE = LOGICAL UNIT     , ACT/S
IST089I A04D8834 TYPE = LOGICAL UNIT     , ACTIV
IST089I A04D8835 TYPE = LOGICAL UNIT     , ACTIV
IST089I A04D8836 TYPE = LOGICAL UNIT     , ACT/S
IST089I A04D8837 TYPE = LOGICAL UNIT     , ACT/S
IST089I A04P885  TYPE = PU_T2            , ACTIV--L--
IST089I A04P886  TYPE = PU_T2            , ACTIV--L--
IST089I A04D8861 TYPE = LOGICAL UNIT     , ACT/S
IST089I A04D8862 TYPE = LOGICAL UNIT     , ACT/S
IST089I A04D8863 TYPE = LOGICAL UNIT     , ACTIV
IST089I A04D8864 TYPE = LOGICAL UNIT     , ACTIV
IST314I END
```

Displaying a channel-attachment major node:

```
d net,id=ctcbc0t3,scope=all
IST097I DISPLAY  ACCEPTED
IST075I NAME = CTCBC0T3         , TYPE = CA MAJOR NODE
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
```

```
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST170I LINES:
IST232I CTCLBC03, ACTIV----E, CUA = BC0
IST314I END
```

Displaying an XCA major node with its subordinate resources:

```
d net,id=xca1a,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = XCA1A, TYPE = XCA MAJOR NODE
IST486I STATUS= ACTIV      , DESIRED STATE= ACTIV
IST1021I MEDIUM=RING,ADAPNO= 1,CUA=0500,SNA SAP= 8
IST1885I SIO = 1234 SLOWDOWN = YES
IST1324I VNNAME =  NETA.CN1           VNGROUP = GP1A2A
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I XCA1A    AC/R    21 NO    902D0000000000000000017100808080
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST170I LINES:
IST232I LN1A2A  , ACTIV
IST232I LN1A7B  , NEVAC
IST232I LN1A9C  , NEVAC
IST232I LN1AAA  , NEVAC
IST232I LN1ABA  , NEVAC
IST232I LN1ACA  , NEVAC
IST232I LN1ADA  , NEVAC
IST232I LN1AEA  , NEVAC
IST314I END
```

Displaying an XCA major node without its subordinate resources:

```
d net,id=x50rbf4a
IST097I DISPLAY ACCEPTED
IST075I NAME = X50RBF4A, TYPE = XCA MAJOR NODE
IST486I STATUS= ACTIV      , DESIRED STATE= ACTIV
IST1021I MEDIUM=RING,ADAPNO= 0,CUA=0BF4,SNA SAP= 4
IST1885I SIO = 1234 SLOWDOWN = YES
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST314I END
```

Displaying an XCA major node that defines a native ATM port:

```
d net,id=xcaosa1a,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = XCAOSA1A, TYPE = XCA MAJOR NODE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1557I MEDIUM = ATM, PORT NAME = OSA11
IST1559I ATM ADDRESS                                    TYPE      FORMAT
IST1553I 11111111111111111111111111111111111111100    LOCAL     NSAP
IST1324I VNNAME = NETA.SSCPVN        VNGROUP = GP1A2AC
IST1559I ATM ADDRESS                                    TYPE      FORMAT
IST1553I 21111111111111111111111111111111111111110    GATEWAY   NSAP
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I XCAOSA1A AC/R    21 NO    1075000000000000000014C00808080
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST170I LINES:
IST232I LN1A2A   ACTIV
IST232I LNP1A2A1 ACTIV
IST232I LN1A2AC1 ACTIV
IST314I END
```

Displaying an XCA major node group that defines a transmission group (TG) to a native ATM connection network:

```
d net,id=gp1a2ac,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = GP1A2AC, TYPE = LINE GROUP
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST231I XCA MAJOR NODE = XCAOSA1A
IST1485I DLCADDR SUBFIELDS FOR GP1A2AC
IST1318I 1,C'ATMSVCNETA.SSCPVNEXCLUSIVE'
IST1318I 7,BCD'03000000 40000000 40000000 536000'
IST1318I 8,X'0003'
IST1318I 21,X'00022111 11111111 11111111 11111111 11111111 1110'
IST084I NETWORK RESOURCES:
IST089I LN1A2AC1 TYPE = LINE             , ACTIV
IST314I END
```

Displaying an XCA major node that defines Enterprise Extender:

```
d net,id=xcaip,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = XCAIP, TYPE = XCA MAJOR NODE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1679I MEDIUM = HPRIP
IST1685I TCP/IP JOB NAME = ***NA***
IST924I-------------------------------------------------------------
IST1324I VNNAME = IP.VNA             VNGROUP = GPVNA     (LOCAL)
IST1910I LOCAL HOSTNAME NODENAME.NETID.DOMAIN
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I XCAIP    NEV      0 NO    107500000000000000000014C00808080
IST924I -------------------------------------------------------------
IST1324I VNNAME = IP.VNB             VNGROUP = GPVNB     (GLOBAL)
IST1680I LOCAL IP ADDRESS 223.254.254.252
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I XCAIP    NEV      0 NO    127500000000000000000014C00808080
IST924I -------------------------------------------------------------
IST1324I VNNAME = IP.VNC             VNGROUP = GPVNC     (GLOBAL)
IST1910I LOCAL HOSTNAME NODENAME.NETID.REALLYREALLYLONGDOMAIN.COM
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I XCAIP    NEV      0 NO    12B400000000000000000017100808080
IST924I -------------------------------------------------------------
IST1902I GROUP = GPIP1
IST1680I LOCAL IP ADDRESS 223.254.254.254
IST924I -------------------------------------------------------------
IST1902I GROUP = GPIP2
IST1680I LOCAL IP ADDRESS 223.254.254.255
IST924I -------------------------------------------------------------
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST170I LINES:
IST1901I LINES UNDER GROUP: GPVNC
IST232I LNIPC1   NEVAC
IST232I LNIPC2   NEVAC
IST1901I LINES UNDER GROUP: GPVNA
IST232I LNIPA1   NEVAC
IST232I LNIPA2   NEVAC
IST1901I LINES UNDER GROUP: GPVNB
IST232I LNIPB1   NEVAC
IST232I LNIPB2   NEVAC
IST232I LNIPB3   NEVAC
IST1901I LINES UNDER GROUP: GPIP1
IST232I LNIP1    NEVAC
IST232I LNIP2    NEVAC
IST1901I LINES UNDER GROUP: GPIP2
IST232I LNIP21   NEVAC
IST232I LNIP22   NEVAC
IST232I LNIP23   NEVAC
IST314I END
```

Displaying a GROUP associated with an XCA major node that defines Enterprise Extender, where the GROUP definition uses only IPADDR to define the IPv4 connection:

```
d net,id=gpip,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = GPIP, TYPE = LINE GROUP
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST231I XCA MAJOR NODE = XCAIP
IST1680I LOCAL IP ADDRESS 223.254.254.252
IST084I NETWORK RESOURCES:
IST089I LNIP1    TYPE = LINE             , NEVAC
IST089I LNIP2    TYPE = LINE             , NEVAC
IST314I END
```

Displaying a GROUP associated with an XCA major node that defines Enterprise Extender, where the GROUP definition uses HOSTNAME to define the IPv6 connection:

```
d net,id=gpip6v,e
IST097I DISPLAY ACCEPTED
IST075I NAME = GPIP6V, TYPE = LINE GROUP
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST231I XCA MAJOR NODE = XCAIP1
IST1680I LOCAL IP ADDRESS 9::67:1:1
IST1910I LOCAL HOSTNAME VIPA26.SSCP1A.RALEIGH.IBM.COM
IST084I NETWORK RESOURCES:
IST089I LNGV6000 TYPE = LINE             , NEVAC
IST089I LNGV6001 TYPE = LINE             , NEVAC
IST314I END
```

Displaying an adjacent CP (CDRSC minor node):

```
d net,id=neta.sscp2a,idtype=cp,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.SSCP2A, TYPE = ADJACENT CP
IST1046I SSCP NETA.SSCP2A ALSO EXISTS
IST486I STATUS= ACT/S----Y, DESIRED STATE= ACTIV - TRACE= OFF
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTCDRDY
IST479I CDRM NAME = SSCP1A, VERIFY OWNER = NO
IST1184I CPNAME = NETA.SSCP2A - NETSRVR = ***NA***
IST1044I ALSLIST = ISTAPNPU
IST082I DEVTYPE = INDEPENDENT LU / CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST171I ACTIVE SESSIONS = 0000000002, SESSION REQUESTS = 0000000002
IST206I SESSIONS:
IST1081I ADJACENT LINK STATION = P3A21
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I SSCP1A   ACTIV/CP-S F6ABEEC38077021A 0002 0001  0  0 NETA
IST635I SSCP1A   ACTIV/CP-P EAABEEC37D76FABF 0001 0002  0  0 NETA
IST314I END
```

Displaying a dependent LU requester:

```
d net,id=nncpa1,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.NNCPA1, TYPE = ADJACENT CP
IST486I STATUS= ACT/S----Y, DESIRED STATE= ACTIV
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=CPSVCMG USS LANGTAB=***NA***
```

```
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTCDRDY
IST1044I ALSLIST = ISTAPNPU
IST1131 DEVICE = ILU/CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST228I ENCRYPTION = OPT, TYPE = TDES24
IST1563I CKEYNAME = NNCPA1 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000004, SESSION REQUESTS = 0000000004
IST206I SESSIONS:
IST1081I ADJACENT LINK STATION = P3A4956K
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I SSCP1A   ACTIV/DL-S E2C5E2E2D6D5000B 001C 0000  0  0 NETA
IST635I SSCP1A   ACTIV/CP-S E2C5E2E2D6D50005 0004 0001  0  0 NETA
IST635I SSCP1A   ACTIV/DL-P EAABEEC3361D945A 0000 0012  0  0 NETA
IST635I SSCP1A   ACTIV/CP-P EAABEEC3361D945B 0001 0005  0  0 NETA
IST1355I PHYSICAL UNITS SUPPORTED BY DLUR NETA.NNCPA1
IST089I AA1PUA   TYPE = PU_T2            , ACTIV
IST089I AA1PUB   TYPE = PU_T2            , ACTIV
IST924I -------------------------------------------------------------
IST075I NAME = NETA.NNCPA1, TYPE = DIRECTORY ENTRY
IST1186I DIRECTORY ENTRY = DYNAMIC NN
IST1184I CPNAME = NETA.NNCPA1 - NETSRVR = ***NA***
IST314I END
```

Displaying an SSCP (CDRM minor node) with virtual-route-based transmission group support:

```
d net,id=neta.sscp2a,idtype=sscp,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.SSCP2A, TYPE = CDRM
IST1046I CP NETA.SSCP2A ALSO EXISTS
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST815I AUTOMATIC RECOVERY IS SUPPORTED
IST231I CDRM  MAJOR NODE = CDRM1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST476I CDRM TYPE = EXTERNAL
IST637I SUBAREA= 2   ELEMENT= 1 SSCPID = 2
IST675I VR = 0, TP = 0
IST389I PREDEFINITION OF CDRSC = OPT
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I SSCP2A   AC/R   255 YES   982D000000000000000017100808080
IST636I CDRSCS OWNED BY SSCP2A   -
IST080I L4A3278A ACTIV      L4A3279A ACTIV      L4A3767D ACTIV
IST080I L4A3278B ACTIV      L4A3279B ACTIV      L4A3287B ACTIV
IST080I L4A3767E ACTIV      L4A4956D ACTIV      L4A4956E ACTIV
IST080I L4A4956F ACTIV      NETAPPL1 ACTIV      NETAPPL2 ACTIV
IST080I NETAPPL3 ACTIV      NETAPPL4 ACTIV      APLMDSEC ACTIV
IST080I TSO2     ACTIV
IST314I END
```

Displaying an SSCP (CDRM) and adjacent CP (CDRSC) with the same name from a network node:

```
d net,id=sscp2a,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.SSCP2A, TYPE = CDRM
IST1046I CP NETA.SSCP2A ALSO EXISTS
IST486I STATUS= NEVAC, DESIRED STATE= INACT - TRACE= OFF
IST815I AUTOMATIC RECOVERY IS SUPPORTED
IST231I CDRM MAJOR NODE = CDRM1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST476I CDRM TYPE = EXTERNAL
IST637I SUBAREA= 2   ELEMENT= 1 SSCPID = 2
IST389I PREDEFINITION OF CDRSC = OPT
IST636I CDRSCS OWNED BY SSCP2A   -
IST080I NETAPPL1 PNF/S
```

```
IST924I -------------------------------------------------------------
IST075I NAME = NETA.SSCP2A, TYPE = ADJACENT CP
IST1046I SSCP NETA.SSCP2A ALSO EXISTS
IST486I STATUS= ACT/S----Y, DESIRED STATE= ACTIV - TRACE= OFF
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTCDRDY
IST479I CDRM NAME = SSCP1A, VERIFY OWNER = NO
IST1184I CPNAME = NETA.SSCP2A - NETSRVR = ***NA***
IST1044I ALSLIST = ISTAPNPU
IST082I DEVTYPE = INDEPENDENT LU / CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST171I ACTIVE SESSIONS = 0000000002, SESSION REQUESTS = 0000000002
IST206I SESSIONS:
IST1081I ADJACENT LINK STATION = P3A21
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I SSCP1A   ACTIV/CP-S F6ABEEC38077021A 0006 0001  0  0 NETA
IST635I SSCP1A   ACTIV/CP-P EAABEEC37D76FABF 0001 0006  0  0 NETA
IST924I -------------------------------------------------------------
IST075I NAME = NETA.SSCP2A, TYPE = DIRECTORY ENTRY
IST1186I DIRECTORY ENTRY = DYNAMIC NN
IST1184I CPNAME = NETA.SSCP2A - NETSRVR = ***NA***
IST314I END
```

Displaying an SSCP (CDRM) and a host CP (application) with the same name:

```
d net,id=neta.sscp1a,idtype=resource,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.SSCP1A, TYPE = CDRM
IST1046I CP NETA.SSCP1A ALSO EXISTS
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST815I AUTOMATIC RECOVERY IS SUPPORTED
IST231I CDRM  MAJOR NODE = VTAMSEG
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST476I CDRM TYPE = HOST, GATEWAY CAPABLE
IST637I SUBAREA= 2   ELEMENT= 1 SSCPID = 2
IST388I DYNAMIC CDRSC DEFINITION SUPPORT = YES
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST172I NO SESSIONS EXIST
IST924I -------------------------------------------------------------
IST075I NAME = NETA.SSCP1A, TYPE = HOST CP
IST1046I SSCP NETA.SSCP1A ALSO EXISTS
IST486I STATUS= ACT/S     , DESIRED STATE= ACTIV
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I APPL  MAJOR NODE = VTAMSEG
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST271I JOBNAME = VTAM    , STEPNAME = VTAM    , DSPNAME = 0AAABIST
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = SSCP1A CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST171I ACTIVE SESSIONS = 0000000002, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I SSCP2A   ACTIV/CP-S EAABEEC3F11FF31F 0002 0001       NETA
IST635I SSCP2A   ACTIV/CP-P F6ABEEC3F4203D93 0001 0002       NETA
IST314I END
```

Displaying the host (this command works for any host). This display shows an interchange node:

```
d net,id=vtam
IST097I DISPLAY ACCEPTED
IST075I NAME = VTAM, TYPE = CDRM
IST1046I CP NETA.SSCP1A ALSO EXISTS
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST599I REAL NAME = NETA.SSCP1A
IST815I AUTOMATIC RECOVERY IS SUPPORTED
IST231I CDRM MAJOR NODE = VTAMSEG
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST2159I XCF GROUP = ISTXCF11 CFS GROUP = ISTCFS11
IST2181I GR STRUCTURE NAME IS ISTGENERIC11
IST2181I MNPS STRUCTURE NAME IS ISTMNPS11
IST476I CDRM TYPE = HOST GATEWAY CAPABLE
IST637I SUBAREA = 1 ELEMENT = 1 SSCPID = 1
IST388I DYNAMIC CDRSC DEFINITION SUPPORT = YES
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST924I -------------------------------------------------------------
IST075I NAME = NETA.SSCP1A, TYPE = HOST CP
IST1046I SSCP NETA.SSCP1A ALSO EXISTS
IST486I STATUS= ACT/S, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = NO
IST1501I XCF TOKEN = 010000B7000F0001
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1632I VPACING = 63
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I APPL MAJOR NODE = VTAMSEG
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST271I JOBNAME = VTAM550T, STEPNAME = NET, DSPNAME = ISTEAF13
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = SSCP1A CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST1633I ASRCVLM = 1999999
IST1634I DATA SPACE USAGE: CURRENT = 0 MAXIMUM = 272
IST171I ACTIVE SESSIONS = 0000000002, SESSION REQUESTS = 0000000000
IST314I END
```

Displaying a CDRSC (no SSCP, adjacent CP, or host CP was found with this name) from a network node:

```
d net,id=neta.netappl1,idtype=resource,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.NETAPPL1, TYPE = CDRSC
IST486I STATUS= ACT/S, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = CDRSC1A
IST479I CDRM NAME = SSCP2A, VERIFY OWNER = NO
IST1184I CPNAME = NETA.SSCP2A - NETSRVR = ***NA***
IST1044I ALSLIST = ISTAPNPU
IST082I DEVTYPE = INDEPENDENT LU / CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = NETAPPL1 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST1081I ADJACENT LINK STATION = P3A21
```

```
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I APPL1    ACTIV-P    EAABEEC356FA371B 0000 0000  0  0 NETA
IST924I -------------------------------------------------------------
IST075I NAME = NETA.NETAPPL1, TYPE = DIRECTORY ENTRY
IST1186I DIRECTORY ENTRY = DYNAMIC LU
IST1184I CPNAME = NETA.SSCP2A - NETSRVR = ***NA***
IST484I SUBAREA = 2
IST1703I DESIRED LOCATE SIZE = 1K LAST LOCATE SIZE = 16K
IST314I END
```

Displaying directory information for a resource (no SSCP, adjacent CP, host CP, or other resource was found with this name) and the command was issued at a network node or interchange node:

```
d net,id=neta.lu71,idtype=resource,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.LU71, TYPE = DIRECTORY ENTRY
IST1186I DIRECTORY ENTRY = DYNAMIC LU
IST1184I CPNAME = NETA.NN3 - NETSRVR = ***NA***
IST484I SUBAREA = ****NA****
IST1703I DESIRED LOCATE SIZE = 1K LAST LOCATE SIZE = 16K
IST314I END
```

Displaying only directory information for a resource:

```
d net,id=sscp2a,idtype=directry,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.SSCP2A, TYPE = DIRECTORY ENTRY
IST1186I DIRECTORY ENTRY = DYNAMIC NN
IST1184I CPNAME = NETA.SSCP2A   - NETSRVR = ***NA***
IST314I END
```

Displaying a conventionally defined application program:

```
d net,id=appl1,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.APPL1, TYPE = APPL
IST486I STATUS= ACT/S, DESIRED STATE= ACTIV - TRACE= OFF
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1632I VPACING =  7
IST1938I APPC = YES
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I APPL MAJOR NODE = APPL1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST271I JOBNAME = ECHO, STEPNAME = ECHO, DSPNAME = IST6D2D6
IST228I ENCRYPTION = OPTIONAL, TYPE = DES
IST1563I CKEYNAME = APPL1 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST1633I ASRCVLM = 2000000
IST1634I DATA SPACE USAGE: CURRENT = 0 MAXIMUM = 0
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000001
IST206I SESSIONS:
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I NETAPPL1 ACTIV-S    EAABEEC37D76FAC1 0000 0000  0  0 NETA
IST314I END
```

Displaying an application program that is multinode persistent session (MNPS) capable:

```
d net,id=mappl1,e
 IST097I DISPLAY ACCEPTED
 IST075I NAME = NETA.MAPPL1, TYPE = DYNAMIC APPL
```

```
 IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
 IST1447I REGISTRATION TYPE = CDSERVR
 IST1550I MNPS STATE = DISABLED
 IST2062I SNPS FORCED TAKEOVER REQUESTS ARE ACCEPTABLE
 IST1629I MODSRCH = NEVER
 IST977I MDLTAB=***NA*** ASLTAB=***NA***
 IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
 IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
 IST1632I VPACING =  7
 IST1938I APPC = NO
 IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
 IST231I APPL MAJOR NODE = APPLANY
 IST1425I DEFINED USING MODEL MAPPL*
 IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
 IST1500I STATE TRACE = OFF
 IST271I JOBNAME = ECHO, STEPNAME = ECHO, DSPNAME = ISTBFA93
 IST228I ENCRYPTION = OPTIONAL , TYPE = DES
 IST1563I CKEYNAME = MAPPL1 CKEY = PRIMARY CERTIFY = NO
 IST1552I MAC = NONE MACTYPE = NONE
 IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
 IST1633I ASRCVLM = 1000000
 IST1634I DATA SPACE USAGE: CURRENT = 0 MAXIMUM = 0
 IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
 IST172I NO SESSIONS EXIST
 IST314I END
```

Displaying an application program that is single node persistent session (SNPS) capable:

```
d net,id=appl1,e
 IST097I DISPLAY ACCEPTED
 IST075I NAME = NETA.APPL1, TYPE = APPL
 IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
 IST1447I REGISTRATION TYPE = CDSERVR
 IST2062I SNPS FORCED TAKEOVER REQUESTS ARE ACCEPTABLE
 IST977I MDLTAB=***NA*** ASLTAB=***NA***
 IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
 IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
 IST1632I VPACING =  7
 IST1938I APPC = NO
 IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
 IST231I APPL MAJOR NODE = APPL1A
 IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
 IST1500I STATE TRACE = OFF
 IST271I JOBNAME = ECHO, STEPNAME = ECHO, DSPNAME = IST4915A
 IST228I ENCRYPTION = OPTIONAL , TYPE = DES
 IST1563I CKEYNAME = APPL1 CKEY = PRIMARY CERTIFY = NO
 IST1552I MAC = NONE MACTYPE = NONE
 IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
 IST1633I ASRCVLM = 1000000
 IST1634I DATA SPACE USAGE: CURRENT = 0 MAXIMUM = 0
 IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
 IST172I NO SESSIONS EXIST
 IST314I END
```

Displaying a model application program:

```
d net,id=appl*,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.APPL*, TYPE = MODEL APPL
IST486I STATUS= CONCT, DESIRED STATE= CONCT - TRACE= OFF
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1938I APPC = NO
IST597I CAPABILITY-PLU INHIBITED,SLU INHIBITED,SESSION LIMIT NON
```

```
IST231I APPL MAJOR NODE = APPL1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST271I JOBNAME = ***NA***, STEPNAME = ***NA***, DSPNAME = ***NA
IST228I ENCRYPTION = OPTIONAL, TYPE = DES
IST1563I CKEYNAME = APPL* CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST1424I APPLICATIONS DEFINED USING THIS MODEL:
IST080I APPL1  ACTIV
IST314I END
```

Displaying a multinode persistent session application program from a remote node connected to the MNPS coupling facility structure might result in any of the following output:

```
d net,id=mapplx1,e
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.MAPPLX1, TYPE = APPL
IST1549I OWNER = NETA.SSCP2A MNPS STATE = DISABLED
IST2062I MNPS FORCED TAKEOVER REQUESTS ARE ACCEPTABLE
IST924I -------------------------------------------------------------
IST075I NAME = NETA.MAPPLX1, TYPE = DIRECTORY ENTRY
IST1186I DIRECTORY ENTRY = REGISTERED LU
IST1184I CPNAME = NETA.SSCP1A - NETSRVR = NETA.SSCPAA
IST314I END
```

```
d net,id=mapplx1,e
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.MAPPLX1, TYPE = CDRSC
IST486I STATUS= ACT/S----Y, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTCDRDY
IST479I CDRM NAME = SSCPAA, VERIFY OWNER = NO
IST1184I CPNAME = NETA.SSCP2A - NETSRVR = ***NA***
IST082I DEVTYPE = INDEPENDENT LU / CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = MAPPLX1 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST1081I ADJACENT LINK STATION = CNR00005
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I APPLAA1  ACTIV-P    EAABEE185A59FD67 0000 0000  0  0 NETA
IST924I -------------------------------------------------------------
IST075I NAME = NETA.MAPPLX1, TYPE = APPL
IST1549I OWNER = NETA.SSCP2A MNPS STATE = ENABLED
IST2062I MNPS FORCED TAKEOVER REQUESTS ARE ACCEPTABLE
IST924I -------------------------------------------------------------
IST075I NAME = NETA.MAPPLX1, TYPE = DIRECTORY ENTRY
IST1186I DIRECTORY ENTRY = DYNAMIC LU
IST1184I CPNAME = NETA.SSCP2A - NETSRVR = ***NA***
IST314I END
```

```
d net,id=mappl1,e
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.MAPPL1, TYPE = CDRSC
IST486I STATUS= ACT/S----Y, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
```

```
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTCDRDY
IST479I CDRM NAME = SSCP1A, VERIFY OWNER = NO
IST1184I CPNAME = NETA.SSCP2A - NETSRVR = ***NA***
IST082I DEVTYPE = INDEPENDENT LU / CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = MAPPL1 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST1081I ADJACENT LINK STATION = CNR00003
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I APPL1    ACTIV-P    EAABEEC30C061090 0000 0000  0  0 NETA
IST924I -------------------------------------------------------------
IST075I NAME = NETA.MAPPL1, TYPE = APPL
IST1549I OWNER = NETA.SSCP2A MNPS STATE = DISABLED
IST2062I MNPS FORCED TAKEOVER REQUESTS ARE ACCEPTABLE
IST314I END
```

```
d net,id=mapplx1,e
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.MAPPLX1, TYPE = APPL
IST486I STATUS= CONCT, DESIRED STATE= CONCT
IST1447I REGISTRATION TYPE = CDSERVR
IST1550I MNPS STATE = DEFINED
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1632I VPACING =  7
IST1938I APPC = YES
IST597I CAPABILITY-PLU INHIBITED,SLU INHIBITED,SESSION LIMIT NONE
IST231I APPL MAJOR NODE = APPLMG2
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST271I JOBNAME = ***NA***, STEPNAME = ***NA***, DSPNAME = ***NA***
IST228I ENCRYPTION = OPTIONAL, TYPE = DES
IST1563I CKEYNAME = MAPPLX1 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST1633I ASRCVLM = 1000000
IST1634I DATA SPACE USAGE: CURRENT = ***NA*** MAXIMUM = ***NA***
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST172I NO SESSIONS EXIST
IST924I -------------------------------------------------------------
IST075I NAME = NETA.MAPPLX1, TYPE = APPL
IST1549I OWNER = NETA.SSCP1A MNPS STATE = DISABLED
IST2062I MNPS FORCED TAKEOVER REQUESTS ARE ACCEPTABLE
IST314I END
```

Displaying a dynamic application program:

```
d net,id=appl1,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.APPL1, TYPE = DYNAMIC APPL
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV - TRACE= OFF
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1632I VPACING =  7
IST1938I APPC = NO
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NON
IST231I APPL MAJOR NODE = APPL1A
IST1425I DEFINED USING MODEL APPL*
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
```

```
IST1500I STATE TRACE = OFF
IST271I JOBNAME = ECHO, STEPNAME = ECHO, DSPNAME = IST75874
IST228I ENCRYPTION = OPTIONAL, TYPE = DES
IST1563I CKEYNAME = APPL1 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST1633I ASRCVLM = 2000000
IST1634I DATA SPACE USAGE: CURRENT = 0 MAXIMUM = 0
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000
IST314I END
```

Displaying the application program representing the network operator:

```
d net,id=istnop
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.ISTNOP, TYPE = APPL
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV - TRACE= OFF
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1395I FLDTAB = ISTMSFLD FILTER = ISTMGC10
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1938I APPC = NO
IST597I CAPABILITY-PLU INHIBITED,SLU INHIBITED,SESSION LIMIT NONE
IST231I APPL MAJOR NODE = VTAMSEG
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST271I JOBNAME = ***NA***, STEPNAME = ***NA***, DSPNAME = ***NA***
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = ISTNOP CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST314I END
```

Displaying a dynamic same-network CDRSC:

```
d net,id=applaa3,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.APPLAA3, TYPE = CDRSC
IST486I STATUS= ACTIV----Y, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTCDRDY
IST479I CDRM NAME = ***NA***, VERIFY OWNER = NO
IST1184I CPNAME = NETA.SSCPAA - NETSRVR = ***NA***
IST082I DEVTYPE = CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = APPLAA3 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST314I END
```

Displaying a dynamic cross-network CDRSC:

```
d net,id=netb.applb11,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETB.APPLB11, TYPE = CDRSC
IST486I STATUS= ACT/S----Y, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
```

```
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTCDRDY
IST479I CDRM NAME = SSCP7B, VERIFY OWNER = NO
IST1184I CPNAME = NETB.SSCP7B - NETSRVR = ***NA***
IST082I DEVTYPE = CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = APPLB11 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000002, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I APPL1    ACTIV-S    C2BB19BC74339803 0016 0016  0  0 NETA
IST635I APPL1    ACTIV-P    EAABEEC34604F7E2 0009 000A  0  0 NETA
IST314I END
```

Displaying a predefined CDRSC for a specific network:

```
d net,id=applb11,netid=netb,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = APPLB11, TYPE = CDRSC
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = CDRSC1A
IST479I CDRM NAME = SSCP7B, VERIFY OWNER = NO
IST082I DEVTYPE = CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = APPLB11 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST314I END
```

Displaying a predefined CDRSC without network (no sessions):

```
d net,id=netappl2,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.NETAPPL2, TYPE = CDRSC
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV - TRACE= OFF
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = CDRSC1A
IST479I CDRM NAME = SSCP2A, VERIFY OWNER = NO
IST082I DEVTYPE = CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST314I END
```

Displaying a model CDRSC:

```
d net,id=applb*,e
IST097I DISPLAY ACCEPTED
IST075I NAME = NETB.APPLB*, TYPE = MODEL CDRSC
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
```

```
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = CDRSC1A
IST2095I MODEL CDRSC DELETE = YES
IST479I CDRM NAME = SSCP7B, VERIFY OWNER = NO
IST082I DEVTYPE = CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST228I ENCRYPTION = NONE , TYPE = DES
IST1563I CKEYNAME = APPLB11 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST2088I CDRSCS DEFINED USING THIS MODEL:
IST483I APPLB11  ACTIV     , CDRM = SSCP7B  , NETID = NETB
IST483I APPLB12  ACTIV     , CDRM = SSCP7B  , NETID = NETB
IST314I END
```

Displaying a clone CDRSC:

```
d net,id=applb11
IST097I DISPLAY ACCEPTED
IST075I NAME = NETB.APPLB11, TYPE = CLONE CDRSC
IST486I STATUS= ACT/S, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = CDRSC1A
IST1425I DEFINED USING MODEL NETB.APPLB*
IST2095I MODEL CDRSC DELETE = YES
IST479I CDRM NAME = SSCP7B, VERIFY OWNER = NO
IST082I DEVTYPE = CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST228I ENCRYPTION = NONE , TYPE = DES
IST1563I CKEYNAME = APPLB11 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST314I END
```

Displaying a CDRSC for a TN3270 or TN3270E client:

```
d net,id=tcpm1011,e
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.TCPM1011, TYPE = CDRSC
IST486I STATUS= ACT/S----Y, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTCDRDY
IST479I CDRM NAME = SSCP1A, VERIFY OWNER = NO
IST1184I CPNAME = NETA.SSCP1A - NETSRVR = ***NA***
IST082I DEVTYPE = CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST228I ENCRYPTION = NONE , TYPE = DES
IST1563I CKEYNAME = TCPM1011 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1727I DNS NAME: VIC127.TCP.RALEIGH.IBM.COM
IST1669I IPADDR..PORT 9.67.113.83..1027
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I TSO20001 ACTIV-P    F6ABEEC39DE3E239 0008 0010  0  0 NETA
IST314I END
```

Displaying a CDRSC that is associated with an IPv6 TN3270 client:

```
d net,id=tcpm2012,e
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.TCPM2012, TYPE = CDRSC
IST486I STATUS= ACT/S----Y, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTCDRDY
IST479I CDRM NAME = SSCP1A, VERIFY OWNER = NO
IST1184I CPNAME = NETA.SSCP1A - NETSRVR = ***NA***
IST1131I DEVICE = CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST228I ENCRYPTION = NONE , TYPE = DES
IST1563I CKEYNAME = TCPM2012 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1669I IPADDR..PORT 2001:0DB8::9:67:115:17..1026
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST634I NAME     STATUS         SID          SEND RECV VR TP NET
IST635I TSO20002 ACTIV-P    F6ABEEC34C26E9F3 0003 000D  0  0 NET
IST314I END
```

Displaying an independent logical unit:

```
d net,id=l3270a,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = L3270A, TYPE = CDRSC
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST599I REAL NAME = ***NA***
IST1447I REGISTRATION TYPE = NO
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST1333I ADJLIST = ***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTPDILU
IST1044I ALSLIST = AHHCPU1
IST082I DEVTYPE = INDEPENDENT LU / CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = L3270A CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST172I NO SESSIONS EXIST
IST924I -------------------------------------------------------------
IST075I NAME = NETA.L3270A, TYPE = DIRECTORY ENTRY
IST1186I DIRECTORY ENTRY = REGISTERED LU
IST1184I CPNAME = NETA.SSCP2A - NETSRVR = NETA.SSCP1A
IST484I SUBAREA = ****NA****
IST1703I DESIRED LOCATE SIZE = 1K LAST LOCATE SIZE = 1K
IST314I END
```

Displaying the host CDRM:

```
d net,id=a01n,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.A01N, TYPE = CDRM
IST1046I CP NETA.A01N ALSO EXISTS
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST815I AUTOMATIC RECOVERY IS SUPPORTED
IST231I CDRM  MAJOR NODE = VTAMSEG
```

```
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST476I CDRM TYPE = HOST, GATEWAY CAPABLE
IST637I SUBAREA= 2   ELEMENT= 1 SSCPID = 2
IST388I DYNAMIC CDRSC DEFINITION SUPPORT = YES
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST172I NO SESSIONS EXIST
IST924I -------------------------------------------------------------
IST075I NAME = NETA.A01N, TYPE = HOST CP
IST1046I SSCP NETA.A01N ALSO EXISTS
IST486I STATUS= ACT/S     , DESIRED STATE= ACTIV
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I APPL  MAJOR NODE = VTAMSEG
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST271I JOBNAME = NET41B  , STEPNAME = NET     , DSPNAME = 00000IST
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST171I ACTIVE SESSIONS = 0000000014, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I A04P882A ACTIV/CP-S E7F3895623BE5C86 000D 0001  0  0 NETY
IST635I A04P888A ACTIV/CP-S E7F3895623BE5C85 053E 0001  0  0 NETA
IST635I A04P886A ACTIV/CP-S E7F3895623BE5C84 0721 0001  0  0 NETA
IST635I A04P885A ACTIV/CP-S E7F3895623BE5C83 03AE 0001  0  0 NETA
IST635I A04P889A ACTIV/CP-S E7F3895623BE5C82 0727 0001  0  0 NETA
IST635I A04P883A ACTIV/CP-S E7F3895623BE5C81 01C5 0001  0  0 NETZ
IST635I A02N     ACTIV/CP-S E7F3895623BE56A5 1055 0001  0  0 NETA
IST635I A02N     ACTIV/CP-P E7E3F9563F1747D7 0001 1047  0  0 NETA
IST635I A04P882A ACTIV/CP-P F3342BAB9019C2B2 0001 000E  0  0 NETY
IST635I A04P883A ACTIV/CP-P E36D478882B602AB 0001 01C6  0  0 NETZ
IST635I A04P885A ACTIV/CP-P EF0E04F6C768DD2E 0001 03AF  0  0 NETA
IST635I A04P886A ACTIV/CP-P EF0E07F6C768E02F 0001 0722  0  0 NETA
IST635I A04P888A ACTIV/CP-P EF0E09F6C768E230 0001 053F  0  0 NETA
IST635I A04P889A ACTIV/CP-P EF0E08F6C768E131 0001 0728  0  0 NETA
IST314I END
```

Displaying an active, same-network, external CDRM:

```
d net,id=A02n,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.A02N, TYPE = CDRM
IST1046I CP NETA.A02N ALSO EXISTS
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST815I AUTOMATIC RECOVERY IS SUPPORTED
IST231I CDRM  MAJOR NODE = A01CDRMC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST476I CDRM TYPE = EXTERNAL
IST637I SUBAREA= 2   ELEMENT= 1 SSCPID = 2
IST675I VR=0, TP=0
IST389I PREDEFINITION OF CDRSC = OPT
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I A02N     AC/R   255 YES   982D000000000000000017100808080
IST1482I HPR= NO - OVERRIDE = YES - CONNECTION = YES
IST636I CDRSCS OWNED BY A02N     -
IST172I NO CDRSCS EXIST
IST924I -------------------------------------------------------------
IST075I NAME = NETA.A02N, TYPE = ADJACENT CP
IST1046I SSCP NETA.A02N ALSO EXISTS
IST486I STATUS= ACT/S----Y, DESIRED STATE= ACTIV
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = ISTCDRDY
IST479I CDRM NAME = A01N    , VERIFY OWNER = NO
```

```
IST1044I ALSLIST = ISTAPNPU
IST082I DEVTYPE = INDEPENDENT LU / CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST171I ACTIVE SESSIONS = 0000000002, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST1081I ADJACENT LINK STATION = A02NETNA
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I A01N     ACTIV/CP-S E7E3F9563F1747D7 1055 0001  0  0 NETA
IST635I A01N     ACTIV/CP-P E7F3895623BE56A5 0001 105F  0  0 NETA
IST924I -------------------------------------------------------------
IST075I NAME = NETA.A02N, TYPE = DIRECTORY ENTRY
IST1186I DIRECTORY ENTRY = DYNAMIC NN
IST1184I CPNAME = NETA.A02N     - NETSRVR = ***NA***
IST314I END
```

Displaying a cross-network external CDRM:

```
d net,id=c01n,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETC.C01N, TYPE = CDRM
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST815I AUTOMATIC RECOVERY IS SUPPORTED
IST231I CDRM  MAJOR NODE = A50CDRMC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST476I CDRM TYPE = EXTERNAL
IST637I SUBAREA= 2   ELEMENT= 1 SSCPID = 2
IST675I VR = 0, TP = 2
IST638I ADJNETSA = 1, ADJNETEL = 1
IST675I VR = 0, TP = 2
IST639I GWN = A0362ZC , ADJNET = NETC
IST640I A500N    ADDR IN ADJNET - SA =         31, EL =    11
IST641I GATEWAY PATH SELECTION LIST -
IST642I  ADJNET     GWN        SUBAREA   ELEM    ADJNETSA  ADJNETEL
IST643I NETC      A0362ZC            3      1           1         1
IST643I NETC                       255      3           1         1
IST898I GWSELECT = YES
IST389I PREDEFINITION OF CDRSC = OPT
IST636I CDRSCS OWNED BY C01N     -
IST080I C01NVLUC ACT/S----Y
IST924I -------------------------------------------------------------
IST075I NAME = NETC.C01N, TYPE = DIRECTORY ENTRY
IST1186I DIRECTORY ENTRY = DYNAMIC EN
IST1184I CPNAME = NETC.C01N     - NETSRVR = NETA.A01N
IST314I END
```

Displaying a peripheral BSC line group:

```
d net,id=a03lbnnb,scope=all
IST097I DISPLAY  ACCEPTED
IST075I NAME = A03LBNNB         , TYPE = LINE GROUP
IST486I STATUS= ACTIV     , DESIRED STATE= ACTIV
IST354I PU T4/5 MAJOR NODE = A0362ZC
IST084I NETWORK NODES:
IST089I A03B00   TYPE = LINE             , NEVAC
IST089I A03C001  TYPE = PU_T2            , NEVAC
IST089I A03C002  TYPE = PU_T2            , NEVAC
IST089I A03B01   TYPE = LINE             , NEVAC
IST089I A03C011  TYPE = PU_T2            , NEVAC
IST089I A03C012  TYPE = PU_T2            , NEVAC
IST089I A03B32   TYPE = LINE             , NEVAC
IST089I A03C321  TYPE = PU_T2            , NEVAC
IST089I A03C322  TYPE = PU_T2            , NEVAC
IST089I A03B33   TYPE = LINE             , NEVAC
IST089I A03C331  TYPE = PU_T2            , NEVAC
IST089I A03C332  TYPE = PU_T2            , NEVAC
IST314I END
```

Displaying a peripheral SDLC line group:

```
d net,id=a03lbnns,scope=all
IST097I DISPLAY  ACCEPTED
IST075I NAME = A03LBNNS         , TYPE = LINE GROUP
IST486I STATUS= ACTIV      , DESIRED STATE= ACTIV
IST354I PU T4/5 MAJOR NODE = A0362ZC
IST084I NETWORK NODES:
IST089I A03S16   TYPE = LINE             , ACTIV
IST089I A03P161  TYPE = PU_T2            , PREQC
IST089I A03P162  TYPE = PU_T2            , PREQC
IST089I A03P163  TYPE = PU_T2            , PREQC
IST089I A03P164  TYPE = PU_T2            , PREQC
IST089I A03S20   TYPE = LINE             , ACTIV
IST075I NAME = A03LBNNS         , TYPE = LINE GROUP
IST089I A03P201  TYPE = PU_T2            , PREQC
IST089I A03P202  TYPE = PU_T2            , PREQC
IST089I A03P203  TYPE = PU_T2            , PREQC
IST089I A03P204  TYPE = PU_T2            , PREQC
IST089I A03P205  TYPE = PU_T2            , PREQC
IST089I A03P206  TYPE = PU_T2            , PREQC
IST314I END
```

Displaying a peripheral SDLC switched line group:

```
d net,id=grp3a9,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = GRP3A9, TYPE = LINE GROUP
IST486I STATUS= ACTIV      , DESIRED STATE= ACTIV
IST354I PU T4/5 MAJOR NODE = NCP3AB5
IST084I NETWORK NODES:
IST089I LN3A9    TYPE = LINE             , ACTIV
IST089I P3A4956K TYPE = PU_T2            , ACTIV--L--
IST089I L3A4956A TYPE = LOGICAL UNIT     , ACT/S
IST089I LN3A10   TYPE = LINE             , ACTIV
IST089I P3A4956L TYPE = PU_T2            , ACTIV--L--
IST089I L3A4956A TYPE = LOGICAL UNIT     , ACT/S
IST089I LN3A11   TYPE = LINE             , ACTIV
IST089I P3A4956M TYPE = PU_T2            , NEVAC
IST314I END
```

Note: Independent LU L3A4956A is shown under two PUs because it has active sessions through these PUs.

Displaying a peripheral BSC link:

```
d net,id=a03b00,scope=all
IST097I DISPLAY  ACCEPTED
IST075I NAME = A03B00           , TYPE = LINE
IST486I STATUS= NEVAC      , DESIRED STATE= INACT
IST087I TYPE = LEASED             , CONTROL = BSC , HPDT = *NA*
IST134I GROUP = A03LBNNB, MAJOR NODE = A0362ZC
IST650I POLL = 000, NEGPOLL = 010, SESSION(S) = 032
IST084I NETWORK NODES:
IST089I A03C001  TYPE = PU_T2            , NEVAC
IST089I A03T0011 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0012 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0013 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0014 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0015 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0016 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0017 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0018 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0019 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T001A TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T001B TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T001C TYPE = LOGICAL UNIT     , NEVAC
```

```
IST089I A03T001D TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T001E TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T001F TYPE = LOGICAL UNIT     , NEVAC
IST089I A03C002  TYPE = PU_T2            , NEVAC
IST089I A03T0021 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0022 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0023 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0024 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0025 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0026 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0027 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0028 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T0029 TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T002A TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T002B TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T002C TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T002D TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T002E TYPE = LOGICAL UNIT     , NEVAC
IST089I A03T002F TYPE = LOGICAL UNIT     , NEVAC
IST314I END
```

Displaying an SDLC link (multidrop INN):

```
d net,id=a04in01,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A04IN01, TYPE = LINE
IST486I STATUS= ACTIV----E , DESIRED STATE = ACTIV
IST087I TYPE = LEASED             , CONTROL = SDLC, HPDT = *NA*
IST134I GROUP = A04MPRI,  MAJOR NODE = A04N43A
IST084I NETWORK NODES:
IST089I A04P013  TYPE = PU_T2            , NEVAC
IST089I A04L013A TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013B TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013C TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013D TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013E TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013F TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013G TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013H TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013I TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013J TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013K TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013L TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013M TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013N TYPE = LOGICAL UNIT     , NEVAC
IST089I A04L013O TYPE = LOGICAL UNIT     , NEVAC
IST089I A04I013A TYPE = LOGICAL UNIT     , NEVAC
IST089I A04I013B TYPE = LOGICAL UNIT     , NEVAC
IST089I A04I013C TYPE = LOGICAL UNIT     , NEVAC
IST089I A04I013D TYPE = LOGICAL UNIT     , NEVAC
IST089I A04I013E TYPE = LOGICAL UNIT     , NEVAC
IST396I LNKSTA    STATUS     CTG GTG ADJNODE  ADJSA  NETID  ADJLS
IST397I A04P014   NEVAC        2   2              0
IST397I A04P015   NEVAC        2   2              0
IST397I A04P016   NEVAC        2   2              0
IST397I A04P017   ACTIV----E   2   2 A31N52B     31
IST397I A04P018   ACTIV----E   2   2 A71N43A     71
IST397I A04P019   NEVAC        2   2              0
IST397I A04P01A   NEVAC        2   2              0
IST397I A04P01B   NEVAC        2   2              0
IST397I A04P01C   NEVAC        2   2              0
IST314I END
```

Displaying a peripheral SDLC link:

```
d net,id=ln3atr10,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = LN3ATR10, TYPE = LINE
```

```
IST486I STATUS= ACTIV      , DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = SDLC, HPDT = *NA*
IST1440I USE = NCP, SPARE RESOURCE, CAN BE REDEFINED
IST134I GROUP = GP3ATRP1, MAJOR NODE = NCP3AB7
IST1324I VNNAME =  NETA.VN1           VNGROUP = GP3ATR10
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I LN3ATR10 AC/R    21 NO    907500000000000000000017100808080
IST084I NETWORK NODES:
IST089I P3ATR10  TYPE = PU_T2            , ACTIV
IST314I END
```

Displaying a cross-subarea SDLC switched link:

```
d net,id=a04hdx00,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A04HDX00, TYPE = LINE
IST486I STATUS= ACTIV      , DESIRED STATE = ACTIV
IST087I TYPE = SWITCHED DIAL-INOUT, CONTROL = SDLC, HPDT = *NA*
IST936I ANSWER MODE = ENABLED
IST134I GROUP = A04SADG1, MAJOR NODE = A04S43A
IST084I NETWORK NODES:
IST089I A31A     TYPE = LINK STATION     , ACTIV
IST314I END
```

Displaying a peripheral SDLC switched link:

```
d net,id=j0004001,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME =J00004001, TYPE = LINE
IST486I STATUS= ACTIV      , DESIRED STATE = ACTIV
IST087I TYPE = SWITCHED DIAL-INOUT, CONTROL = SDLC, HPDT = *NA*
IST936I ANSWER MODE = ENABLED
IST134I GROUP = A04TRLG1, MAJOR NODE = A04S43A
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST172I NO NETWORK NODES EXIST
IST314I END
```

Displaying an NTRI line in an NCP:

```
d net,id=ln3atr11
IST097I DISPLAY ACCEPTED
IST075I NAME = LN3ATR11, TYPE = LINE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = SWITCHED DIAL-INOUT, CONTROL = SDLC, HPDT = *NA*
IST936I ANSWER MODE = ENABLED
IST1440I USE = NCP, DEFINED RESOURCE, CANNOT BE REDEFINED
IST134I GROUP = GP3ATR10, MAJOR NODE = NCP3AB8
IST1500I STATE TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - NO
IST1657I MAJOR NODE VTAMTOPO = IGNORE
IST314I END
```

Displaying a logical line in an XCA major node:

```
d net,id=ln1a2a
IST097I DISPLAY ACCEPTED
IST075I NAME = LN1A2A, TYPE = LINE
IST486I STATUS= NEVAC, DESIRED STATE= INACT
IST087I TYPE = SWITCHED DIAL-INOUT, CONTROL = SDLC, HPDT = *NA*
IST936I ANSWER MODE = RESET
IST134I GROUP = GP1A2A, MAJOR NODE = XCA1A
IST1500I STATE TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST1657I MAJOR NODE VTAMTOPO = REPORT
IST314I END
```

Displaying XCF TRLE:

```
d net,id=istt1q2q,e
IST097I DISPLAY ACCEPTED
IST075I NAME = ISTT1Q2Q, TYPE = TRLE
IST1954I TRL MAJOR NODE = ISTTRL
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = XCF , HPDT = *NA*
IST1715I MPCLEVEL = HPDT       MPCUSAGE = SHARE
IST1717I ULPID = ISTP1Q2Q ULP INTERFACE = *NA*
IST1503I XCF TOKEN = 0200001900120002     STATUS = ACTIVE
IST1502I ADJACENT CP = NETA.SSCP2A
IST1500I STATE TRACE = OFF
IST314I END
```

Displaying TCP TRLE:

```
d net,id=iutx0aa0
IST097I DISPLAY ACCEPTED
IST075I NAME = IUTX0AA0, TYPE = TRLE
IST1954I TRL MAJOR NODE = ISTTRL
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = TCP , HPDT = *NA*
IST1717I ULPID = TCPCS ULP INTERFACE = *NA*
IST1221I READ  DEV = 0AA0 STATUS = ACTIVE     STATE = N/A
IST1221I WRITE DEV = 0AA1 STATUS = ACTIVE     STATE = N/A
IST1500I STATE TRACE = OFF
IST314I END
```

Displaying internal shared memory (ISM) TRLE:

```
d net,id=iut00011
IST097I DISPLAY ACCEPTED
IST075I NAME = IUT00011, TYPE = TRLE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = *NA*               , CONTROL = ISM, HPDT = *NA*
IST1954I TRL MAJOR NODE = ISTTRL
IST2418I SMCD PFID = 0011  VCHID = 0140  PNETID = ZOSNET
IST2417I VFN = 0001
IST924I -------------------------------------------------------------
IST1717I ULPID = TCPIP2 ULP INTERFACE = EZAISM02
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1500I STATE TRACE = OFF
IST314I END
```

Displaying a 10GbE RoCE Express TRLE in a dedicated RoCE environment:

```
d net,id=iut10005
IST097I DISPLAY ACCEPTED
IST075I NAME = IUT10005, TYPE = TRLE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = *NA*               , CONTROL = ROCE, HPDT = *NA*
IST1954I TRL MAJOR NODE = ISTTRL
IST2361I SMCR PFID = 0005  PCHID = 0500  PNETID = NETWORK3
IST2362I PORTNUM = 1  RNIC CODE LEVEL = 2.10.4750
IST2389I PFIP = 01000300
IST924I -------------------------------------------------------------
IST1717I ULPID = TCPIP1 ULP INTERFACE = EZARIUT10005
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1500I STATE TRACE = OFF
IST1866I TRLE = IUT10005   INOPDUMP = ON
IST924I -----------------------------------------------------
IST1717I ULPID = TCPIP2 ULP INTERFACE = EZARIUT10005
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1500I STATE TRACE = OFF
IST1866I TRLE = IUT10005   INOPDUMP = ON
IST314I END
```

Displaying a 10GbE RoCE Express TRLE in a shared RoCE environment:

```
d net,id=iut10011
IST097I DISPLAY ACCEPTED
IST075I NAME = IUT10011, TYPE = TRLE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = *NA*               , CONTROL = ROCE, HPDT = *NA*
IST1954I TRL MAJOR NODE = ISTTRL
IST2361I SMCR PFID = 0011  PCHID = 0140  PNETID = PNETID1
IST2362I PORTNUM = 1  RNIC CODE LEVEL = **NA**
IST2389I PFIP = 01000300
IST2417I VFN = 0001
IST924I -------------------------------------------------------------
IST1717I ULPID = TCPIP2 ULP INTERFACE = EZARIUT10011
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1500I STATE TRACE = OFF
IST314I END
```

Displaying a switched major node:

```
d net,id=swxca1a,e
IST097I DISPLAY ACCEPTED
IST075I NAME = SWXCA1A, TYPE = SW SNA MAJ NODE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST084I NETWORK RESOURCES:
IST089I SW1A2A   TYPE = PU_T2            , CONCT
IST089I SW1A7B   TYPE = PU_T2            , CONCT
IST089I SW1A9C   TYPE = PU_T2            , CONCT
IST089I SW1AAA   TYPE = PU_T2            , CONCT
IST089I SW1ABA   TYPE = PU_T2            , CONCT
IST089I SW1ACA   TYPE = PU_T2            , CONCT
IST089I SW1ADA   TYPE = PU_T2            , CONCT
IST089I SW1AEA   TYPE = PU_T2            , CONCT
IST1500I STATE TRACE = OFF
IST314I END
```

Displaying a switched PU in this switched major node:

```
d net,id=sw1a2a
IST097I DISPLAY ACCEPTED
IST075I NAME = SW1A2A, TYPE = PU_T2
IST486I STATUS= CONCT, DESIRED STATE= CONCT
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = YES - FINAL USE = NOT FINAL
IST136I SWITCHED SNA MAJOR NODE = SWXCA1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST1656I VTAMTOPO = NOREPORT, NODE REPORTED - YES
IST1657I MAJOR NODE VTAMTOPO = INCLUDE
IST314I END
```

Displaying a cross-subarea SDLC link:

```
d net,id=a04c08,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A04C08, TYPE = LINE
IST486I STATUS= NEVAC      , DESIRED STATE= INACT
IST087I TYPE = LEASED             , CONTROL = SDLC, HPDT = *NA*
IST134I GROUP = A04XCA0,  MAJOR NODE = A0462ZC
IST396I LNKSTA    STATUS     CTG GTG ADJNODE  ADJSA  NETID  ADJLS
IST397I A04P08A   NEVAC        1   1             0
IST314I END
```

Displaying a cross-subarea channel link:

```
d net,id=012-l,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = 012-L, TYPE = LINE
```

```
IST486I STATUS= ACTIV----I , DESIRED STATE = ACTIV
IST087I TYPE = LEASED            , CONTROL = NCP , HPDT = *NA*
IST134I GROUP = ISTGROUP, MAJOR NODE = A99MPU
IST396I LNKSTA    STATUS     CTG GTG ADJNODE  ADJSA  NETID  ADJLS
IST397I 012-S     ACTIV----I   1   1 A03N43A      3
IST314I END
```

Displaying a cross-subarea channel link station:

```
d net,id=012-s,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = 012-S, TYPE = LINK STATION
IST486I STATUS= ACTIV----I , DESIRED STATE = ACTIV
IST081I LINE NAME = 012-L, LINE GROUP = ISTGROUP, MAJNOD = A99MPU
IST396I LNKSTA    STATUS     CTG GTG ADJNODE  ADJSA  NETID  ADJLS
IST397I 012-S     ACTIV----I   1   1 A03N43A      3
IST610I                            LINE 012-L    - STATUS ACTIV----I
IST314I END
```

Displaying a cross-subarea SDLC link station:

```
d net,id=a03p644,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A03P644, TYPE = LINK STATION
IST486I STATUS= NEVAC      , DESIRED STATE = INACT
IST081I LINE NAME = A03IN64, LINE GROUP = A03MPRI, MAJNOD = A03N43A
IST396I LNKSTA    STATUS     CTG GTG ADJNODE  ADJSA  NETID  ADJLS
IST397I A03P644   NEVAC        2   2              0
IST610I                            LINE A03IN64  - STATUS NEVAC
IST314I END
```

Displaying a cross-subarea XCA link station with ALLOWACT=YES coded:

```
d net,id=pu1a12,e
IST097I DISPLAY ACCEPTED
IST075I NAME = PU1A12, TYPE = LINK STATION
IST486I STATUS= ACTIV--W-E, DESIRED STATE= ACTIV
IST081I LINE NAME = LN1A12, LINE GROUP = GP1AS, MAJNOD = XCA1A
IST1500I STATE TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST1657I MAJOR NODE VTAMTOPO = REPORT
IST396I LNKSTA   STATUS     CTG GTG  ADJNODE ADJSA    NETID    ADJLS
IST397I PU1A12   ACTIV--W-E   1   1    NCP12    12     NETA   PU121A
IST610I                            LINE LN1A12   - STATUS ACTIV----E
IST314I END
```

Displaying a physical unit:

```
d net,id=a03p011,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A03P011, TYPE = PU_T2.1
IST486I STATUS= ACTIV      , DESIRED STATE = ACTIV
IST2238I DISCNT = NO - FINAL USE = *NA*
IST081I LINE NAME = A03IN01, LINE GROUP = A03MPRI, MAJNOD = A03N43A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST355I LOGICAL UNITS:
IST080I A03L011A NEVAC      A03L011B NEVAC      A03L011C NEVAC
IST080I A03L011D NEVAC      A03L011E NEVAC      A03L011F NEVAC
IST080I A03L011G NEVAC      A03L011H NEVAC      A03L011I NEVAC
IST080I A03L011J NEVAC      A03L011K NEVAC      A03L011L NEVAC
IST080I A03L011M NEVAC      A03L011N NEVAC      A03L011O NEVAC
IST314I END
```

Displaying a physical unit with APPN host-to-host connectivity:

```
d net,id=ahhcpu1
IST097I DISPLAY ACCEPTED
IST075I NAME = AHHCPU1, TYPE = PU_T2.1
```

```
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = YES - FINAL USE = FINAL
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I AHHCPU1  AC/R    21 YES   988D000000000000000014C00808080
IST1482I HPR = RTP - OVERRIDE = N/A - CONNECTION = YES
IST1510I LLERP = REQUIRED - RECEIVED = REQUIRED
IST136I LOCAL SNA MAJOR NODE = LSAHHC1
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST1314I TRLE = TRLE1A    STATUS = ACTIV       CONTROL = MPC
IST314I END
```

Displaying a physical unit with DLUR support:

```
d net,id=aa1pua,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = AA1PUA, TYPE = PU_T2
IST486I STATUS= ACTIV      , DESIRED STATE= ACTIV
IST1043I CP NAME = ***NA***, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = NO
IST2238I DISCNT = YES - FINAL USE = NOT FINAL
IST1354I DLUR NAME = NNCPA1             MAJNODE = SWDLR1A
IST136I SWITCHED SNA MAJOR NODE = SWDLR1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST355I LOGICAL UNITS:
IST080I AA1LUA1  ACT/S      AA1LUA2  ACTIV      AA1LUA3  ACTIV
IST080I AA1LUA4  ACTIV
IST314I END
```

Displaying a Rapid Transport Protocol (RTP) physical unit:

```
d net,id=cnr00004
IST097I DISPLAY ACCEPTED
IST075I NAME = CNR00004, TYPE = PU_T2.1
IST486I STATUS= ACTIV--LX-, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = DELAY - FINAL USE = FINAL
IST1392I DISCNTIM = 00010 DEFINED AT PU FOR DISCONNECT
IST2178I RPNCB ADDRESS = 126FCA18
IST1963I APPNCOS = #INTER - PRIORITY = HIGH
IST1476I TCID X'1239C4D900000014' - REMOTE TCID X'1239D9D700000016'
IST1481I DESTINATION CP NETA.SSCP2A - NCE X'D000000000000000'
IST1587I ORIGIN NCE X'D000000000000000'
IST1966I ACTIVATED AS ACTIVE ON 05/30/03 AT 09:40:30
IST2237I CNR00004 CURRENTLY REPRESENTS A LIMITED RESOURCE
IST1477I ALLOWED DATA FLOW RATE = 355 KBITS/SEC
IST1516I INITIAL DATA FLOW RATE = 1600 KBITS/SEC
IST1841I ACTUAL DATA FLOW RATE = 85 KBITS/SEC
IST1511I MAXIMUM NETWORK LAYER PACKET SIZE = 16410 BYTES
IST1478I NUMBER OF UNACKNOWLEDGED BUFFERS = 0
IST1479I RTP CONNECTION STATE = CONNECTED - MNPS = NO
IST1959I DATA FLOW STATE: NORMAL
IST1855I NUMBER OF SESSIONS USING RTP = 372
IST1697I RTP PACING ALGORITHM = ARB RESPONSIVE MODE
IST1480I RTP END TO END ROUTE - RSCV PATH
IST1460I TGN  CPNAME             TG TYPE      HPR
IST1461I  21  NETA.SSCP2A        APPN         RTP
IST875I ALSNAME TOWARDS RTP = AHHCPU1
IST1738I ANR LABEL               TP           ER NUMBER
IST1739I 8001000A00000000        *NA*         *NA*
IST231I RTP MAJOR NODE = ISTRTPMN
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = ON, OPTION = PU
IST314I END
```

Tip: The REMOTE TCID shown on message IST1476I can be used to correlate a local RTP PU name to the RTP PU name used by the remote (VTAM) partner RTP node (shown on the IST1481I message) to represent the same RTP connection. To determine the RTP PU name used by the remote (VTAM) partner RTP node, first issue the above command on the local node and remember the REMOTE TCID value from the IST1476I message. Then issue the DISPLAY RTPS,TCID=tcid command on the remote (VTAM) partner RTP node using the REMOTE TCID value from the prior display.

Displaying a Rapid Transport Protocol (RTP) physical unit with additional diagnostic information:

```
D NET,ID=CNR00004,HPRDIAG=YES
IST097I DISPLAY ACCEPTED
IST075I NAME = CNR00004, TYPE = PU_T2.1
IST486I STATUS= ACTIV--LX-, DESIRED STATE= ACTIV
IST2244I HPRDIAG DISPLAY ISSUED ON 10/14/08 AT 09:42:17
IST1043I CP NAME = SSCP2A - CP NETID = NETA - DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = DELAY - FINAL USE = FINAL
IST1392I DISCNTIM = 00010 DEFINED AT PU FOR DISCONNECT
IST231I RTP MAJOR NODE = ISTRTPMN
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST2178I RPNCB ADDRESS 06639018
IST1963I APPNCOS = #INTER - PRIORITY = HIGH
IST1476I TCID X'246F137A0001000E' - REMOTE TCID X'246F178B0001000E'
IST1481I DESTINATION CP NETA.SSCP2A - NCE X'D000000000000000'
IST1587I ORIGIN NCE X'D000000000000000'
IST1966I ACTIVATED AS ACTIVE ON 10/14/08 AT 09:34:22
IST1479I RTP CONNECTION STATE = CONNECTED - MNPS = NO
IST1959I DATA FLOW STATE = NORMAL
IST1855I NUMBER OF SESSIONS USING RTP = 10
IST1480I RTP END TO END ROUTE - RSCV PATH
IST1460I TGN  CPNAME             TG TYPE      HPR
IST1461I  21  NETA.SSCP2A        APPN         RTP
IST875I ALSNAME TOWARDS RTP = AHHCPU1
IST1738I ANR LABEL               TP           ER NUMBER
IST1739I 8001000A00000000        *NA*         *NA*
IST924I -------------------------------------------------------------
IST1968I ARB INFORMATION:
IST1844I ARB MODE = GREEN
IST1697I RTP PACING ALGORITHM = ARB RESPONSIVE MODE
IST1477I ALLOWED DATA FLOW RATE = 1600 KBITS/SEC
IST1516I INITIAL DATA FLOW RATE = 1600 KBITS/SEC
IST1841I ACTUAL DATA FLOW RATE = 146 KBITS/SEC
IST1969I MAXIMUM ACTUAL DATA FLOW RATE = 164 KBITS/SEC
IST1862I ARB MAXIMUM SEND RATE = 32 MBITS/SEC
IST1846I CURRENT RECEIVER THRESHOLD = 36850 MICROSECONDS
IST1846I MAXIMUM RECEIVER THRESHOLD = 37000 MICROSECONDS
IST1846I MINIMUM RECEIVER THRESHOLD = 17000 MICROSECONDS
IST1970I RATE REDUCTIONS DUE TO RETRANSMISSIONS = 0
IST924I -------------------------------------------------------------
IST1971I TIMER INFORMATION:
IST1852I LIVENESS TIMER = 180 SECONDS
IST1851I SMOOTHED ROUND TRIP TIME = 9 MILLISECONDS
IST1972I SHORT REQUEST TIMER = 250 MILLISECONDS
IST2229I REFIFO TIMER = 68 MILLISECONDS
IST924I -------------------------------------------------------------
IST1973I OUTBOUND TRANSMISSION INFORMATION:
IST1974I NUMBER OF NLPS SENT = 173104 ( 173K )
IST1975I TOTAL BYTES SENT = 16055969 ( 16M )
IST1849I LARGEST NLP SENT = 140 BYTES
IST1980I SEQUENCE NUMBER = 8265162 (X'007E1DCA')
IST1842I NUMBER OF NLPS RETRANSMITTED = 0
IST2249I NLP RETRANSMIT RATE = 0.0000%
```

```
IST1976I BYTES RETRANSMITTED = 0 ( 0K )
IST1478I NUMBER OF UNACKNOWLEDGED BUFFERS = 1
IST1958I NUMBER OF ORPHANED BUFFERS = 0
IST1843I NUMBER OF NLPS ON WAITING-TO-SEND QUEUE = 0
IST1847I NUMBER OF NLPS ON WAITING-FOR-ACKNOWLEDGEMENT QUEUE = 1
IST2268I NUMBER OF BYTES ON WAITING-FOR-ACK QUEUE = 15
IST1977I MAXIMUM NUMBER OF NLPS ON WAITING-FOR-ACK QUEUE = 19
IST2269I MAXIMUM NUMBER OF BYTES ON WAITING-FOR-ACK QUEUE = 879
IST1978I WAITING-FOR-ACK QUEUE MAX REACHED ON 10/14/08 AT 09:34:22
IST2085I NUMBER OF NLPS ON OUTBOUND WORK QUEUE = 0
IST2086I MAXIMUM NUMBER OF NLPS ON OUTBOUND WORK QUEUE = 20
IST2087I OUTBOUND WORK QUEUE MAX REACHED ON 10/14/08 AT 09:34:22
IST1511I MAXIMUM NETWORK LAYER PACKET SIZE = 16410 BYTES
IST924I -------------------------------------------------------------
IST1979I INBOUND TRANSMISSION INFORMATION:
IST2059I NUMBER OF NLPS RECEIVED = 184391 ( 184K )
IST1981I TOTAL BYTES RECEIVED = 16696275 ( 16M )
IST1850I LARGEST NLP RECEIVED = 104 BYTES
IST1980I SEQUENCE NUMBER = 8480224 (X'008165E0')
IST1853I NUMBER OF NLPS ON OUT-OF-SEQUENCE QUEUE = 0
IST2230I MAXIMUM NUMBER OF NLPS ON OUT-OF-SEQUENCE QUEUE = 0
IST1854I NUMBER OF NLPS ON INBOUND SEGMENTS QUEUE = 0
IST1982I NUMBER OF NLPS ON INBOUND WORK QUEUE = 0
IST1983I MAXIMUM NUMBER OF NLPS ON INBOUND WORK QUEUE = 27
IST924I -------------------------------------------------------------
IST1984I PATH SWITCH INFORMATION:
IST2271I PATH SWITCH DELAY = 0
IST1856I LAST PATH SWITCH OCCURRENCE WAS ON 10/14/08 AT 09:34:59
IST1937I PATH SWITCH REASON: INITIATED BY REMOTE PARTNER
IST1985I PATH SWITCHES INITIATED FROM REMOTE RTP = 1
IST1986I PATH SWITCHES INITIATED FROM LOCAL RTP = 0
IST1987I PATH SWITCHES DUE TO LOCAL FAILURE = 0
IST1988I PATH SWITCHES DUE TO LOCAL PSRETRY = 0
IST924I -------------------------------------------------------------
IST1857I BACKPRESSURE REASON COUNTS:
IST1858I PATHSWITCH  SEND QUEUE MAX  STORAGE FAILURE  STALLED PIPE
IST2205I ----------  --------------  ---------------  ------------
IST1859I      0             0               0              0
IST2211I ACK QUEUE MAX
IST2205I -------------
IST2212I      0
IST924I -------------------------------------------------------------
IST2250I ALL DIAGNOSTIC COUNTERS CLEARED ON 10/14/08 AT 09:34:22
IST314I END
```

Displaying a Rapid Transport Protocol (RTP) physical unit with the diagnostic information and clearing the diagnostic counters:

```
D NET,ID=CNR00004,HPRDIAG=YES,CLEAR=ALL
IST097I DISPLAY ACCEPTED
IST075I NAME = CNR00004, TYPE = PU_T2.1
IST486I STATUS= ACTIV--LX-, DESIRED STATE= ACTIV
IST2244I HPRDIAG DISPLAY ISSUED ON 10/14/08 AT 09:43:53
IST1043I CP NAME = SSCP2A - CP NETID = NETA - DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = DELAY - FINAL USE = FINAL
IST1392I DISCNTIM = 00010 DEFINED AT PU FOR DISCONNECT
IST231I RTP MAJOR NODE = ISTRTPMN
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST2178I RPNCB ADDRESS 06639018
IST1963I APPNCOS = #INTER - PRIORITY = HIGH
IST1476I TCID X'246F137A0001000E' - REMOTE TCID X'246F178B0001000E'
IST1481I DESTINATION CP NETA.SSCP2A - NCE X'D000000000000000'
IST1587I ORIGIN NCE X'D000000000000000'
IST1966I ACTIVATED AS ACTIVE ON 10/14/08 AT 09:34:21
IST1479I RTP CONNECTION STATE = CONNECTED - MNPS = NO
```

```
IST1959I DATA FLOW STATE = NORMAL
IST1855I NUMBER OF SESSIONS USING RTP = 10
IST1480I RTP END TO END ROUTE - RSCV PATH
IST1460I TGN  CPNAME             TG TYPE      HPR
IST1461I  21  NETA.SSCP2A        APPN         RTP
IST875I ALSNAME TOWARDS RTP = AHHCPU1
IST1738I ANR LABEL               TP           ER NUMBER
IST1739I 8001000A00000000        *NA*         *NA*
IST924I -------------------------------------------------------------
IST1968I ARB INFORMATION:
IST1844I ARB MODE = GREEN
IST1697I RTP PACING ALGORITHM = ARB RESPONSIVE MODE
IST1477I ALLOWED DATA FLOW RATE = 1600 KBITS/SEC
IST1516I INITIAL DATA FLOW RATE = 1600 KBITS/SEC
IST1841I ACTUAL DATA FLOW RATE = 148 KBITS/SEC
IST1969I MAXIMUM ACTUAL DATA FLOW RATE = 164 KBITS/SEC
IST1862I ARB MAXIMUM SEND RATE = 32 MBITS/SEC
IST1846I CURRENT RECEIVER THRESHOLD = 36850 MICROSECONDS
IST1846I MAXIMUM RECEIVER THRESHOLD = 37000 MICROSECONDS
IST1846I MINIMUM RECEIVER THRESHOLD = 17000 MICROSECONDS
IST1970I RATE REDUCTIONS DUE TO RETRANSMISSIONS = 0
IST924I -------------------------------------------------------------
IST1971I TIMER INFORMATION:
IST1852I LIVENESS TIMER = 180 SECONDS
IST1851I SMOOTHED ROUND TRIP TIME = 9 MILLISECONDS
IST1972I SHORT REQUEST TIMER = 250 MILLISECONDS
IST2229I REFIFO TIMER = 68 MILLISECONDS
IST924I -------------------------------------------------------------
IST1973I OUTBOUND TRANSMISSION INFORMATION:
IST1974I NUMBER OF NLPS SENT = 210394 ( 210K )
IST1975I TOTAL BYTES SENT = 19553353 ( 19M )
IST1849I LARGEST NLP SENT = 140 BYTES
IST1980I SEQUENCE NUMBER = 10044954 (X'0099461A')
IST1842I NUMBER OF NLPS RETRANSMITTED = 0
IST2249I NLP RETRANSMIT RATE = 0.0000%
IST1976I BYTES RETRANSMITTED = 0 ( 0K )
IST1478I NUMBER OF UNACKNOWLEDGED BUFFERS = 1
IST1958I NUMBER OF ORPHANED BUFFERS = 0
IST1843I NUMBER OF NLPS ON WAITING-TO-SEND QUEUE = 0
IST1847I NUMBER OF NLPS ON WAITING-FOR-ACKNOWLEDGEMENT QUEUE = 1
IST2268I NUMBER OF BYTES ON WAITING-FOR-ACK QUEUE = 15
IST1977I MAXIMUM NUMBER OF NLPS ON WAITING-FOR-ACK QUEUE = 19
IST2269I MAXIMUM NUMBER OF BYTES ON WAITING-FOR-ACK QUEUE = 879
IST1978I WAITING-FOR-ACK QUEUE MAX REACHED ON 10/14/08 AT 09:34:21
IST2085I NUMBER OF NLPS ON OUTBOUND WORK QUEUE = 0
IST2086I MAXIMUM NUMBER OF NLPS ON OUTBOUND WORK QUEUE = 20
IST2087I OUTBOUND WORK QUEUE MAX REACHED ON 10/14/08 AT 09:34:21
IST1511I MAXIMUM NETWORK LAYER PACKET SIZE = 16410 BYTES
IST924I -------------------------------------------------------------
IST1979I INBOUND TRANSMISSION INFORMATION:
IST2059I NUMBER OF NLPS RECEIVED = 224100 ( 224K )
IST1981I TOTAL BYTES RECEIVED = 20319156 ( 20M )
IST1850I LARGEST NLP RECEIVED = 104 BYTES
IST1980I SEQUENCE NUMBER = 10306550 (X'009D43F6')
IST1853I NUMBER OF NLPS ON OUT-OF-SEQUENCE QUEUE = 0
IST2230I MAXIMUM NUMBER OF NLPS ON OUT-OF-SEQUENCE QUEUE = 0
IST1854I NUMBER OF NLPS ON INBOUND SEGMENTS QUEUE = 0
IST1982I NUMBER OF NLPS ON INBOUND WORK QUEUE = 0
IST1983I MAXIMUM NUMBER OF NLPS ON INBOUND WORK QUEUE = 27
IST924I -------------------------------------------------------------
IST1984I PATH SWITCH INFORMATION:
IST2271I PATH SWITCH DELAY = 0
IST1856I LAST PATH SWITCH OCCURRENCE WAS ON 10/14/08 AT 09:34:59
IST1937I PATH SWITCH REASON: INITIATED BY REMOTE PARTNER
IST1985I PATH SWITCHES INITIATED FROM REMOTE RTP = 1
IST1986I PATH SWITCHES INITIATED FROM LOCAL RTP = 0
IST1987I PATH SWITCHES DUE TO LOCAL FAILURE = 0
```

```
IST1988I PATH SWITCHES DUE TO LOCAL PSRETRY = 0
IST924I -------------------------------------------------------------
IST1857I BACKPRESSURE REASON COUNTS:
IST1858I PATHSWITCH  SEND QUEUE MAX  STORAGE FAILURE  STALLED PIPE
IST2205I ----------  --------------  ---------------  ------------
IST1859I      0             0                0              0
IST2211I ACK QUEUE MAX
IST2205I -------------
IST2212I      0
IST924I -------------------------------------------------------------
IST2250I ALL DIAGNOSTIC COUNTERS CLEARED ON 10/14/08 AT 09:34:21
IST2248I ALL DIAGNOSTIC COUNTERS CLEARED FOR 1 RTP PIPES
IST314I END
```

Displaying an HPR-capable PU:

```
d net,id=ahhcpu1
IST097I DISPLAY ACCEPTED
IST075I NAME = AHHCPU1, TYPE = PU_T2.1
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = YES - FINAL USE = NOT FINAL
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I AHHCPU1  AC/R    21 YES   988D000000000000000014C00808080
IST1482I HPR = RTP - OVERRIDE = N/A - CONNECTION = YES
IST1510I LLERP = REQUIRED - RECEIVED = REQUIRED
IST136I LOCAL SNA MAJOR NODE = LSAHHC1
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST1314I TRLE = TRLE1A    STATUS = ACTIV       CONTROL = MPC
IST314I END
```

Displaying a switched link station:

```
d net,id=swpux2a1,e
IST097I DISPLAY ACCEPTED
IST075I NAME = SWPUX2A1, TYPE = PU_T2.1
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = DELAY - FINAL USE = NOT FINAL
IST1392I DISCNTIM = 00010 DEFINED AT PU FOR DISCONNECT
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I SWPUX2A1 AC/R    22 YES   982D000000000000000017100808080
IST1482I HPR = NONE - OVERRIDE = N/A - CONNECTION = NO
IST136I SWITCHED SNA MAJOR NODE = SWND3AB8
IST081I LINE NAME = LN3AXN11, LINE GROUP = GP3AXN10, MAJNOD = NCP3AB8
IST1068I PHYSICAL RESOURCE (PHYSRSC) = P3AXN10
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST1656I VTAMTOPO = NOREPORT, NODE REPORTED - YES
IST1657I MAJOR NODE VTAMTOPO = INCLUDE
IST172I NO LOGICAL UNITS EXIST
IST314I END
```

Displaying a switched PU type 2:

```
d net,id=a04p501,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A04P501, TYPE = PU_T2
IST486I STATUS= CONCT      , DESIRED STATE = CONCT
IST2238I DISCNT = YES - FINAL USE = NOT FINAL
IST136I SWITCHED SNA MAJOR NODE = A04SG1
IST1934I  IDBLK = 002   IDNUM = 02345
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST1657I MAJOR NODE VTAMTOPO = INCLUDE
```

```
IST355I LOGICAL UNITS:
IST080I A04L501A CONCT      A04L501B CONCT      A04L501C CONCT
IST080I A04L501D CONCT      A04L501E CONCT      A04L501F CONCT
IST080I A04L501G CONCT      A04L501H CONCT      A04L501I CONCT
IST080I A04L501J CONCT      A04L501K CONCT      A04L501L CONCT
IST080I A04L501M CONCT      A04L501N CONCT      A04L501O CONCT
IST314I END
```

Displaying a switched PU type 2.1 (LAN capable):

```
D NET,ID=SOE10302,scope=all
IST097I DISPLAY  ACCEPTED
IST075I NAME = SOE10302         , TYPE = PU_T2.1
IST486I STATUS= ACTIV--LX-, DESIRED STATE= ACTIV
IST1058I MODEL LU GROUP = LUGR    , LUSEED =
IST1043I CP NAME = SOE10301, CP NETID = GBSOEL00, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = NO - FINAL USE = *NA*
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I SOE10302 AC/R    21 YES   9875000000000000000014C00808080
IST1482I HPR = NONE - OVERRIDE = N/A - CONNECTION = NO
IST956I PU   SAP=  4 MAC=000524E10156 MAXDATA= 1437
IST1935I RIF = 0AB000011910100210050
IST136I SWITCHED SNA MAJOR NODE = ISTDSWMN
IST081I LINE NAME = L530217D, LINE GROUP = G5302   , MAJNOD = SOE53F02
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST1656I VTAMTOPO = REPORT  , NODE REPORTED - YES
IST1657I MAJOR NODE VTAMTOPO = REPORT
IST355I LOGICAL UNITS:
IST080I SOE1030I ACTIV---X- SOE1030J ACTIV---X- SOE1030K ACTIV---X-
IST314I END
```

Displaying a switched PU type 2.1 (AS/400):

```
d net,id=a04p882,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A04P882, TYPE = PU_T2.1
IST486I STATUS= ACTIV--L-- , DESIRED STATE= ACTIV
IST1043I CP NAME = A04P882A, CP NETID = NETY, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = NO - FINAL USE = *NA*
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I A04P882  AC/R    21 YES   802D000000000000000017100000000
IST136I SWITCHED SNA MAJOR NODE = A04SMNC
IST081I LINE NAME = J000401B, LINE GROUP = A04BLG1, MAJNOD = A0462ZC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST355I LOGICAL UNITS:
IST080I A04I8823 ACT/S      A04I8822 ACT/S      A04P882A ACT/S----Y
IST080I A04I8821 ACT/S
IST314I END
```

Displaying a local SNA physical unit:

```
d net,id=pua,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = PUA, TYPE = PU_T2
IST486I STATUS = ACTIV      , DESIRED STATE= ACTIV
IST2238I DISCNT = YES - FINAL USE = FINAL
IST136I LOCAL    SNA MAJOR NODE = A50LSNA
IST077I SIO = *NA*  CUA = 0770
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST355I LOGICAL UNITS:
IST080I LSNALU1  ACTIV      LSNALU2  ACTIV      LSNALU3  ACTIV
IST080I LSNALU4  ACTIV
IST314I END
```

Displaying a dynamic XCF local SNA physical unit:

```
d net,id=istp0001,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = ISTP0001, TYPE = PU_T2.1
IST486I STATUS= ACTIV--LX-, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = NO - FINAL USE = *NA*
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I ISTP0001 AC/R    21 YES   988D000000000000000014C0080808
IST1482I HPR = NONE - OVERRIDE = N/A - CONNECTION = NO
IST136I LOCAL SNA MAJOR NODE = ISTLSXCF
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST1314I TRLE = ISTT0001  STATUS = ACTIV----E  CONTROL = XCF
IST355I LOGICAL UNITS:
IST080I SSCP2A   ACT/S----Y
IST314I END
```

Displaying a dynamic XCF local SNA physical unit, specifying the control point name:

```
d net,id=sscp2a,idtype=xcfcp
IST097I DISPLAY ACCEPTED
IST075I NAME = ISTP0001, TYPE = PU_T2.1
IST486I STATUS= ACTIV--LX-, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = YES - FINAL USE = NOT FINAL
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I ISTP0001 AC/R    21 YES   988D000000000000000014C00808080
IST1482I HPR = NONE - OVERRIDE = N/A - CONNECTION = NO
IST136I LOCAL SNA MAJOR NODE = ISTLSXCF
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST1314I TRLE = ISTT0001  STATUS = ACTIV----E  CONTROL = XCF
IST314I END
```

Displaying a logical unit under an NCP:

```
d net,id=a04dxxx1,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.A04DXXX1, TYPE = LOGICAL UNIT
IST486I STATUS= NEVAC----T , DESIRED STATE= INACT
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU INHIBITED,SLU INHIBITED,SESSION LIMIT 00000001
IST081I LINE NAME = A04VXX, LINE GROUP = A04XNPAX, MAJNOD = A0462ZC
IST135I PHYSICAL UNIT = A04NXXX
IST082I DEVTYPE = LU
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST172I NO SESSIONS EXIST
IST314I END
```

Displaying a switched logical unit:

```
d net,id=a31d0711,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = A31D0711, TYPE = LOGICAL UNIT
IST486I STATUS= NEVAC      , DESIRED STATE= INACT
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=CRYPTLOG USSTAB=AUSSTAB LOGTAB=INTERP
IST934I DLOGMOD=REQENCRP USS LANGTAB=***NA***
```

```
IST597I CAPABILITY-PLU INHIBITED,SLU INHIBITED,SESSION LIMIT 00000001
IST136I SWITCHED SNA MAJOR NODE = SMNDDNN
IST135I PHYSICAL UNIT = A31P021
IST082I DEVTYPE = LU
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1936I LOCADDR = 003
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST172I NO SESSIONS EXIST
IST314I END
```

Displaying a local SNA logical unit:

```
d net,id=lsnalu1,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.LSNALU1, TYPE = LOGICAL UNIT
IST486I STATUS= ACTIV      , DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=AMODETAB USSTAB=AUSSTAB LOGTAB=***NA***
IST934I DLOGMOD=D4A32782 USS LANGTAB=***NA***
IST597I CAPABILITY-PLU INHIBITED,SLU INHIBITED,SESSION LIMIT 00000001
IST136I LOCAL    SNA MAJOR NODE = A50LSNA
IST135I PHYSICAL UNIT = PUA , CUA = 0770
IST082I DEVTYPE = LU
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1936I LOCADDR = 003
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST172I NO SESSIONS EXIST
IST314I END
```

Displaying a local non-SNA logical unit:

```
d net,id=a50a721,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.A50A721, TYPE = LOGICAL UNIT
IST486I STATUS= ACT/S      , DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=AMODETAB USSTAB=AUSSTAB LOGTAB=INTERP
IST934I DLOGMOD=M23270I  USS LANGTAB=***NA***
IST597I CAPABILITY-PLU INHIBITED,SLU ENABLED  ,SESSION LIMIT 00000001
IST351I LOCAL 3270 MAJOR NODE = A50LOCAL
IST077I SIO = 00010 CUA = 0721
IST1131I DEVICE = LU
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000001
IST206I SESSIONS:
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I ECHOC1C  ACTIV-P    D73BC0750F6AE8F3 0000 0001  0  0 NETC
IST635I ECHO50B  PREALC-P   ECC39EEE2AA3BC6E                 NETA
IST314I END
```

Displaying a native ATM permanent virtual channel (PVC):

```
d net,id=lnp1a2a1,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = LNP1A2A1, TYPE = LINE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = SDLC, HPDT = *NA*
IST1554I PVCNAME = PV11211
IST134I GROUP = GPP1A1, MAJOR NODE = XCAOSA1A
IST1500I STATE TRACE = OFF
IST084I NETWORK RESOURCES:
IST089I PP1A2A1  TYPE = PU_T2.1          , ACTIV
IST314I END
```

Displaying a remote node connected through a native ATM PVC:

```
d net,id=pp1a2a1,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = PP1A2A1, TYPE = PU_T2.1
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = NO - FINAL USE = *NA*
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I PP1A2A1  AC/R    21 YES   182D0000000000000000017100808080
IST1482I HPR = RTP - OVERRIDE = N/A - CONNECTION = YES
IST1510I LLERP = REQUIRED - RECEIVED = REQUIRED
IST1555I VPCI/VCI = 010100
IST081I LINE NAME = LNP1A2A1, LINE GROUP = GPP1A1, MAJNOD = XCAOSA1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST172I NO LOGICAL UNITS EXIST
IST314I END
```

Displaying a remote node connected through a native ATM switched virtual channel (SVC):

```
d net,id=sw1a2a,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = SW1A2A, TYPE = PU_T2.1
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = NO - FINAL USE = *NA*
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I SW1A2A   AC/R    22 YES   182D0000000000000000017100808080
IST1482I HPR = RTP - OVERRIDE = N/A - CONNECTION = YES
IST1510I LLERP = REQUIRED - RECEIVED = REQUIRED
IST1559I ATM ADDRESS                                    TYPE      FORMAT
IST1553I 11111111111111111111111111111111111111100    LOCAL     NSAP
IST1553I 21111111111111111111111111111111111111110    REMOTE    NSAP
IST1555I VPCI/VCI = 010200
IST136I SWITCHED SNA MAJOR NODE = SWXCA1A
IST081I LINE NAME = LN1A2A, LINE GROUP = GP1A2A, MAJNOD = XCAOSA1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST1656I VTAMTOPO = NOREPORT, NODE REPORTED - YES
IST1657I MAJOR NODE VTAMTOPO = INCLUDE
IST355I LOGICAL UNITS:
IST080I SW1A2AL  NEVAC
IST314I END
```

Displaying a remote node connected through Enterprise Extender when the connection uses IPv4 addresses without host names:

```
d net,id=sw1a2a,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = SW1A2A, TYPE = PU_T2.1
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = NO - FINAL USE = *NA*
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I SW1A2A AC/R 22 YES 182D0000000000000000017100808080
IST1482I HPR = RTP - OVERRIDE = N/A - CONNECTION = YES
IST1510I LLERP = REQUIRED - RECEIVED = REQUIRED
IST1680I LOCAL IP ADDRESS 9.18.100.2
IST1680I REMOTE IP ADDRESS 223.254.254.1
IST2114I LIVTIME:    INITIAL = 10   MAXIMUM =  0   CURRENT = 10
IST136I SWITCHED SNA MAJOR NODE = SWXCA1
IST081I LINE NAME = LN1A2A, LINE GROUP = GP1A2A, MAJNOD = XCAHPR1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
```

```
IST1500I STATE TRACE = OFF
IST355I LOCAL UNITS:
IST080I SW1A2AL NEVAC
IST314I END
```

Displaying a remote node connected through Enterprise Extender when the connection uses IPv6 addresses:

```
d net,id=sw1a26a,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = SW1A26A, TYPE = PU_T2.1
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = NO - FINAL USE = *NA*
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I SW1A26A AC/R 22 YES 182D0000000000000000017100808080
IST1482I HPR = RTP - OVERRIDE = N/A - CONNECTION = YES
IST1510I LLERP = REQUIRED - RECEIVED = REQUIRED
IST1680I LOCAL IP ADDRESS 3FFE::9.18.100.2
IST1910I LOCAL HOSTNAME LOCALHOST.DOMAIN.COM
IST1680I REMOTE IP ADDRESS 3FFC:1001:1002:3451:7223:2254:4254:4441
IST1909I REMOTE HOSTNAME REMOTEHOST.DOMAIN.COM
IST2114I LIVTIME:    INITIAL = 10   MAXIMUM =  0   CURRENT = 10
IST136I SWITCHED SNA MAJOR NODE = SWXCA1
IST081I LINE NAME = LN1A26A, LINE GROUP = GP1A26A,MAJNOD = XCAHPR1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST355I LOCAL UNITS:
IST080I SW1A2A6L NEVAC
IST314I END
```

Displaying a remote node connected through Enterprise Extender when the connection uses IPv4 addresses:

```
d net,id=sw1a26b,scope=all
IST097I DISPLAY ACCEPTED
IST075I NAME = SW1A26B, TYPE = PU_T2.1
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = NO - FINAL USE = *NA*
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I SW1A26B AC/R 22 YES 182D0000000000000000017100808080
IST1482I HPR = RTP - OVERRIDE = N/A - CONNECTION = YES
IST1510I LLERP = REQUIRED - RECEIVED = REQUIRED
IST1680I LOCAL IP ADDRESS 9.18.100.2
IST1910I LOCAL HOSTNAME LOCALHOST2.DOMAIN.COM
IST1680I REMOTE IP ADDRESS 09.26.130.4
IST2114I LIVTIME:    INITIAL = 10   MAXIMUM =  0   CURRENT = 10
IST136I SWITCHED SNA MAJOR NODE = SWXCA1
IST081I LINE NAME = LN1A26B, LINE GROUP = GP1A26B, MAJNOD = XCAHPR1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST355I LOCAL UNITS:
IST080I SW1A2B6L NEVAC
IST314I END
```

Displaying a dynamic Enterprise Extender PU:

```
d net,id=e2000018
IST097I DISPLAY ACCEPTED
IST075I NAME = E2000018, TYPE = PU_T2.1
IST486I STATUS= ACTIV---X-, DESIRED STATE= ACTIV
IST1043I CP NAME = SSCP2A - CP NETID = NETA - DYNAMIC LU = YES
IST1589I XNETALS = YES
IST2238I DISCNT = NO - FINAL USE = *NA*
```

```
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I E2000018 AC/R     5 YES   98750000000000000000017100808080
IST1482I HPR = RTP - OVERRIDE = N/A - CONNECTION = YES
IST1510I LLERP = NOTPREF - RECEIVED = NOTALLOW
IST1680I LOCAL IP ADDRESS 9.67.1.1
IST1910I LOCAL HOSTNAME VIPA14.SSCP1A
IST1680I REMOTE IP ADDRESS 9.67.1.2
IST2114I LIVTIME:    INITIAL =   10   MAXIMUM =    0   CURRENT =   10
IST136I SWITCHED SNA MAJOR NODE = ISTDSWMN
IST081I LINE NAME = LNEE2000, LINE GROUP = GPEE2, MAJNOD = XCAEE2
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST1657I MAJOR NODE VTAMTOPO = REPORT
IST314I END
```

Displaying a resource name that is known in several networks:

```
d net,id=*.applb12,max=3
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.APPLB12, TYPE = APPL
IST486I STATUS= CONCT      , DESIRED STATE= CONCT
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1938I APPC = NO
IST597I CAPABILITY-PLU INHIBITED,SLU INHIBITED,SESSION LIMIT NONE
IST231I APPL  MAJOR NODE = APPL1A
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST271I JOBNAME = ***NA***, STEPNAME = ***NA***, DSPNAME = ***NA***
IST228I ENCRYPTION = OPTIONAL, TYPE = DES
IST1563I CKEYNAME = APPLB12 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST924I -------------------------------------------------------------
IST075I NAME = NETB.APPLB12, TYPE = CDRSC
IST486I STATUS= ACTIV      , DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1632I VPACING = 7
IST1938I APPC = NO
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = CDRSC1A
IST479I CDRM NAME = SSCP7B  , VERIFY OWNER = NO
IST1131I DEVICE = CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST228I ENCRYPTION = NONE, TYPE = DES
IST1563I CKEYNAME = APPLB12 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST924I -------------------------------------------------------------
IST075I NAME = NETC.APPLB12, TYPE = CDRSC
IST486I STATUS= ACTIV      , DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = CDSERVR
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I CDRSC MAJOR NODE = CDRSC1A
IST479I CDRM NAME = SSCP9C  , VERIFY OWNER = NO
IST1131I DEVICE = CDRSC
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST228I ENCRYPTION = NONE, TYPE = DES
```

```
IST1563I CKEYNAME = APPLB12 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST171I ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST314I END
```

Displaying a generic resource:

```
d net,id=GRAPPL,idtype=generic
IST097I DISPLAY ACCEPTED
IST075I NAME = GRAPPL, TYPE = GENERIC RESOURCE
IST1359I MEMBER NAME        OWNING CP   SELECTABLE  APPC
IST1360I NETA.NETAPPL1      SSCP2A          YES       NO
IST1360I NETA.APPL1         SSCP1A          NO        NO
IST1360I NETA.APPLAA1       SSCPAA          DEL       NO
IST2210I GR PREFERENCE TABLE ENTRY = **NAMELESS**
IST2202I GREXIT   = YES      WLM      = YES      LOCLU  = YES
IST2204I LOCAPPL  = YES      PASSOLU  = YES
IST1393I GENERIC RESOURCE NAME RESOLUTION EXIT IS ISTEXCGR
IST314I END
```

Displaying an IP address in dotted decimal format when there is only one TN3270 client connected at this IP address:

```
d net,idtype=ipaddr,ID=9.67.113.58
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.TCPM1001, TYPE = APPL
IST486I STATUS= ACT/S, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = CDSERVR
IST599I REAL NAME = NETA.TCPM1001
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=ISTINCLM USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1632I VPACING =  7
IST1938 APPC = YES
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT 00000001
IST231I APPL MAJOR NODE = TCPAPPLS
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST271I JOBNAME = TCPCS, STEPNAME = TCPCS, DSPNAME = ISTD629B
IST228I ENCRYPTION = OPTIONAL, TYPE = DES
IST1563I CKEYNAME = TCPM1001 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST1633I ASRCVLM = 1000000
IST1634I DATA SPACE USAGE: CURRENT = 0 MAXIMUM = 0
IST1669I IPADDR..PORT 9.67.113.58..1029
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST314I END
```

Displaying an IP address in colon-hexadecimal format when there is only one TN3270 client connected at this IPv6 address.

```
d net,id=2001:0DB8::9:67:115:17,idtype=ipaddr
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.TCPM2013, TYPE = DYNAMIC APPL
IST486I STATUS= ACT/S, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = CDSERVR
IST599I REAL NAME = NETA.TCPM2013
IST1629I MODSRCH = NEVER
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=ISTINCLM USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1632I VPACING =  7
IST1938I APPC = YES
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT 00000001
IST231I APPL MAJOR NODE = TCPAPPLS
IST1425I DEFINED USING MODEL TCPM*
```

```
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST271I JOBNAME = TCPCS, STEPNAME = TCPCS, DSPNAME = ISTF27CE
IST228I ENCRYPTION = OPTIONAL , TYPE = DES
IST1563I CKEYNAME = TCPM2013 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST1633I ASRCVLM = 1000000
IST1634I DATA SPACE USAGE: CURRENT = 0 MAXIMUM = 0
IST1669I IPADDR..PORT 2001:0DB8::9:67:115:17..1027
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST314I END
```

Displaying a resource with TN3270 characteristics.

```
d net,id=tcpm2013
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.TCPM2013, TYPE = DYNAMIC APPL
IST486I STATUS= ACT/S, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = CDSERVR
IST1629I MODSRCH = NEVER
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=ISTINCLM USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1632I VPACING =  7
IST1938I APPC = YES
IST597I CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT 00000001
IST231I APPL MAJOR NODE = TCPAPPLS
IST1425I DEFINED USING MODEL TCPM*
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST271I JOBNAME = TCPCS, STEPNAME = TCPCS, DSPNAME = ISTF27CE
IST228I ENCRYPTION = OPTIONAL , TYPE = DES
IST1563I CKEYNAME = TCPM2013 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST1633I ASRCVLM = 1000000
IST1634I DATA SPACE USAGE: CURRENT = 0 MAXIMUM = 0
IST1669I IPADDR..PORT 2001:0DB8::9:67:115:17..1027
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST314I END
```

Displaying an IP address with multiple TN3270 client connections.

```
d net,id=2001:0DB8::9:67:115:17,idtype=ipaddr

IST097I DISPLAY ACCEPTED
IST1912I IP ADDRESS 2001:0DB8::9:67:115:17 102
IST1913I LUNAME            PORT
IST1914I NETA.TCPM2013     1027
IST1914I NETA.TCPM2012     1026
IST314I END
```

Displaying a TSO user ID when the SLU is a Telnet client:

```
d net,tsouser,id=user1
IST097I DISPLAY ACCEPTED
IST075I NAME = USER1, TYPE = TSO USERID
IST486I STATUS= ACTIV, DESIRED STATE= N/A
IST576I TSO TRACE = OFF
IST262I ACBNAME = TSO0003, STATUS = ACT/S
IST262I LUNAME = TCPM1002, STATUS = ACT/S
IST1669I IPADDR..PORT 2001:0DB8::9:67:115:17..1026
IST2203I CHARACTER SET 0065 CODE PAGE 0025
IST314I END
```

Displaying a DLUR CDRSC:

```
d net,id=NNP7
IST075I  NAME = D7NET.NNP7       , TYPE = ADJACENT CP
IST486I  STATUS= ACT/S----Y, DESIRED STATE= ACTIV
IST1402I      SRTIMER = 30           SRCOUNT = 100
IST1447I  REGISTRATION TYPE = NO
IST977I  MDLTAB=***NA*** ASLTAB=***NA***
IST1333I  ADJLIST = ***NA***
IST861I  MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I  DLOGMOD=CPSVCMG  USS LANGTAB=***NA***
IST597I  CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I  CDRSC    MAJOR NODE = ISTCDRDY
IST1184I  CPNAME = D7NET.NNP7        - NETSRVR = ***NA***
IST1044I  ALSLIST = ISTAPNPU
IST1131I  DEVICE = ILU/CDRSC
IST654I  I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I  STATE TRACE = OFF
IST171I  ACTIVE SESSIONS = 0000000003, SESSION REQUESTS = 0000000000
IST206I  SESSIONS:
IST1081I  ADJACENT LINK STATION = PBB7N10
IST634I  NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I  CDRMD730 ACTIV/CP-P F8B7DBABF0AB700C 0001 015D  0  0 D7NET
IST1355I  PHYSICAL UNITS SUPPORTED BY DLUR D7NET.NNP7
IST089I  D779AP1  TYPE = PU_T2            , PAPU2
IST924I  ------------------------------------------------------------
IST075I        NAME=D7NET.NNP7       ,TYPE=DIRECTORY ENTRY
IST1186I      DIRECTORY ENTRY = DYNAMIC  NN
IST1184I      CPNAME = D7NET.NNP7           -NETSRVR = ***NNA***
IST1402I       SRTIMER = 30           SRCOUNT = 100
IST134I        END
```

DISPLAY INOPDUMP command

Purpose

The DISPLAY INOPDUMP command is used to determine:

- The global status for INOPDUMP. The global status controls the INOPDUMP function for resources that are not defined within a transport resource list entry (TRLE). When a TRLE is activated, the global status is propagated to the newly activated TRLE if the TRLE InOpDump status has not been explicitly set.
- Whether TRLE controlled resources are subject to INOPDUMP and, if so, the TRLE names.
- Whether TRLEs subsequently activated, whose InOpDump status has not been explicitly set, will be subject to INOPDUMP.

Resulting display

The resulting display shows:

- The global status for INOPDUMP
- The names of all TRL major nodes having at least one TRLE currently having INOPDUMP set to ON.
- TRLEs that currently have INOPDUMP set to ON (TRLEs that currently have INOPDUMP=OFF are not displayed)

Examples

Displaying INOPDUMP information when the INOPDUMP status of specific TRLEs is ON, but the global INOPDUMP status is OFF:

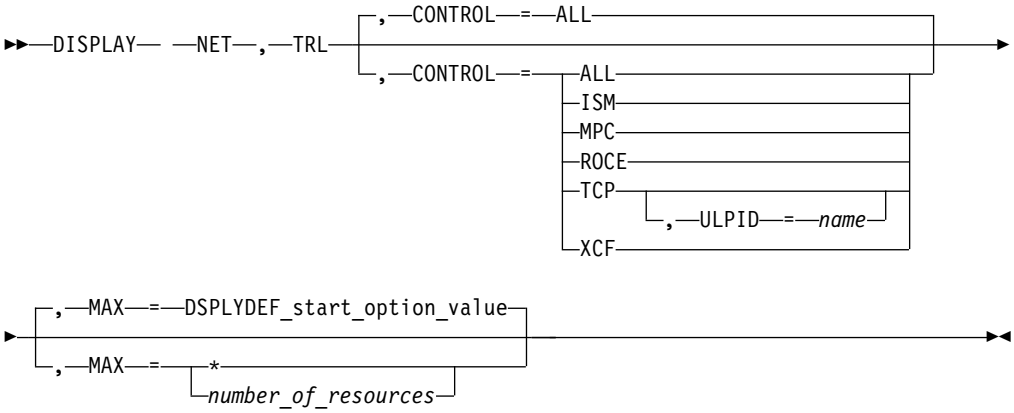
```
d net,inopdump
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = INOPDUMP
IST1865I GLOBAL INOPDUMP = OFF
IST924I ------------------------------
IST1954I TRL MAJOR NODE = TRL1A
IST1866I TRLE = TRLE1A   INOPDUMP = ON
IST1866I TRLE = TRLE1B   INOPDUMP = ON
IST924I ------------------------------
IST1954I TRL MAJOR NODE = TRL1B
IST1866I TRLE = TRLE1F   INOPDUMP = ON
IST314I END
```

Displaying INOPDUMP information when the INOPDUMP status of one or more INOPDUMP control groups is ON:

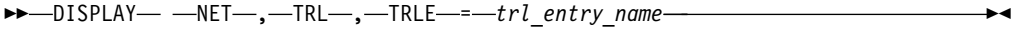
```
d net,inopdump
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = INOPDUMP
IST1865I GLOBAL INOPDUMP = ON BY CONTROL GROUPS
IST1904I INOPDUMP = (IQDIO,ISM,ROCE)
IST924I ------------------------------------------------------------
IST1954I TRL MAJOR NODE = ISTTRL
IST1866I TRLE = IUT00051   INOPDUMP = ON
IST1866I TRLE = IUT1A004   INOPDUMP = ON
IST1866I TRLE = IUT1A003   INOPDUMP = ON
IST1866I TRLE = IUTIQDIO   INOPDUMP = ON
IST314I END
```

DISPLAY TRL command

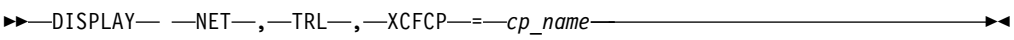
Display the entries in the TRL major nodes:



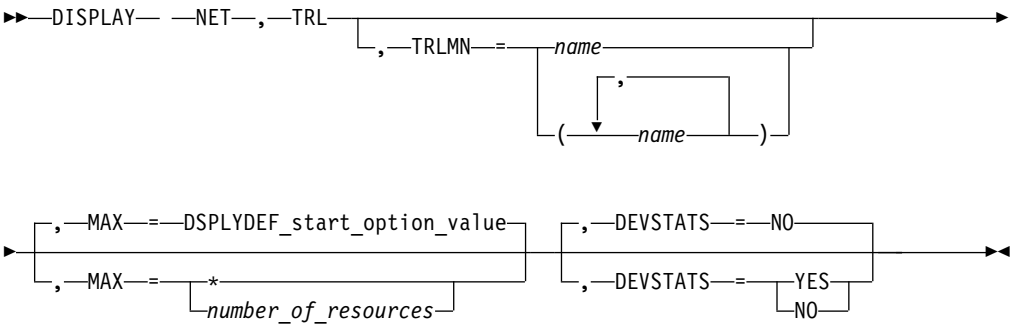
Display information about a specific user-defined TRLE:



Display information about a dynamic XCF TRLE:



Display the entries in one or more specific TRL major nodes:



Abbreviations

Operand	Abbreviation
DISPLAY	D
DEVSTATS=YES	DEVSTATS

Purpose

The DISPLAY TRL (transport resource list) command provides information about the active TRL major nodes or about a single TRLE (transport resource list entry).

Operands

CONTROL
Specifies the type of connections to display.

CONTROL=ALL
Specifies that information is to be displayed about all TRLEs.

CONTROL=ISM
Specifies that information is to be displayed about internal shared memory (ISM) TRLEs only.

CONTROL=MPC
Specifies that information is to be displayed about user-defined TRLEs only.

CONTROL=RoCE
Specifies that information is to be displayed about RDMA over Converged Ethernet (RoCE) TRLEs only.

CONTROL=TCP
Specifies that information is to be displayed about dynamic TCP/IP TRLEs only.

CONTROL=XCF
Specifies that information is to be displayed about dynamic XCF TRLEs only.

DEVSTATS
Specifies whether statistics for RoCE TRLEs should be collected and displayed. This operand is meaningful only when the TRLE operand is also specified, and the value that is specified for the TRLE operand represents a RoCE TRLE; otherwise, the operand is ignored.

DEVSTATS=YES
Specifies that statistics should be collected for the RoCE TRLE.

DEVSTATS=NO
Specifies that statistics should not be collected for the RoCE TRLE. This is the default setting.

MAX
Specifies the maximum number of TRLEs that VTAM displays for this command.

If you specify the MAX operand, do not specify TRLE.

MAX=*
Specifies that the value of the DSPLYMAX start option is used to limit the display output.

MAX=number_of_resources
Specifies the number of TRLEs to display for this command. The valid range is 1 - value of DSPLYMAX. The default is the value specified for the DSPLYDEF start option.

Specifying MAX limits the display output. VTAM searches only for the number of instances that you have specified. When that number is found, VTAM does not search any further. This saves processing time for the command and gives you control over the amount of display output generated by the command. If fewer TRLEs are found than you have specified on MAX, VTAM displays only the TRLEs that are found.

TRLE=trl_entry_name
Specifies the name of the TRLE to be displayed.

TRLMN=trl_major_node_name
Specifies the name of one or more active TRL major nodes to be displayed.

ULPID=name
Specifies the name of a CS z/OS upper-layer protocol (ULP) to be displayed, for example, the TCP/IP procedure name. The ULPID operand is valid only with CONTROL=TCP.

XCFCP=cp_name
Specifies that information is to be displayed about the TRLE representing the connection to another VTAM in the XCF group. The value of *cp_name* is the CP name or SSCP name of the other VTAM.

Resulting display

The resulting display shows:

- The name and status of all TRLEs in the active TRL major nodes if the TRLE operand is not specified.
- The name and status of the TRLE specified on the TRLE operand. If the status is active and the TRLE is not associated with a 10 GbE RoCE Express interface, the display also includes the address and operational status of the READ, WRITE, and (OSA-Express and HiperSockets only) DATA subchannels. In addition, the following information may be displayed:

  - MPC level and usage (MPC header size, maximum MPC data size, inbound data storage medium)
  - Name of the CS z/OS upper-layer protocols (ULPs) using this TRLE
  - OSA portname, OSA adapter number, and OSA microcode level
  - OSA or HiperSockets channel path id (chpid) type and number
  - Physical channel ID (PCHID) for the 10GbE RoCE Express feature
  - Virtual channel ID (VCHID) for the internal shared memory (ISM) device
  - Physical network ID (PNetID) for the 10GbE RoCE Express feature and ISM device
  - Peripheral Component Interconnect Express (PCIe) function ID (PFID) for the 10GbE RoCE Express feature and ISM device
    - When the RoCE Express feature is operating in a dedicated RoCE environment, the 10GbE RoCE Express microcode level is displayed.
    - When the feature is operating in a shared RoCE environment, the virtual function number (VFN) is displayed.
  - Microcode level when a 10GbE RoCE Express feature is operating in a dedicated RoCE environment
  - Virtual function number (VFN) for an ISM device or a 10GbE RoCE Express feature that operates in a shared RoCE environment
  - I/O trace status
  - The capability of the connection to perform channel I/O directly to or from communications storage manager (CSM) buffers
  - Storage information about the inbound and outbound queues associated with the DATA subchannels
- For a dynamic TCP TRLE, an exclusively owned TRLE, or an ISM TRLE, only one message with a ULP ID is issued because only one ULP can use each of these TRLEs. For an OSA-Express adapter, one message with a ULP ID is issued for each datapath channel address that a ULP uses. For other TRLEs, more than one ULP ID message can be issued, depending on how many ULPs are using the TRLE.

  Rule: Only one message with a ULP ID is generated for a 10GbE RoCE Express feature that operates in a shared RoCE environment.
- The ULP ID will be the jobname for TCP/IP ULPs, the SNA PU name for ANNC ULPs, and the XCA Major Node name for ATM or EE ULPs.
- Message group IST2396I is generated after the base TRL information is displayed when DEVSTATS=YES is specified and the TRLE that is specified on the TRLE operand represents a 10 GbE RoCE Express interface. See z/OS Communications Server: SNA Messages for specifics on the statistics reported in the IST2396I message group.

Examples

Displaying all TRL entries:

```
d net,trl
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = TRL
IST1954I TRL MAJOR NODE = ISTTRL
IST1314I TRLE = ISTT0001  STATUS = ACTIVE----E   CONTROL = XCF
IST1454I 1 TRLE(S) DISPLAYED
IST924I -------------------------------------------------------------
IST1954I TRL MAJOR NODE = TRL1
IST1314I TRLE = TRL1A  STATUS = ACTIVE  CONTROL = MPC
```

```
IST1314I TRLE = TRL1B  STATUS = NEVAC   CONTROL = MPC
IST1454I 2 TRLE(S) DISPLAYED
IST924I -------------------------------------------------------
IST1954I TRL MAJOR NODE = TRL2
IST1314I TRLE = TRL2A  STATUS = NEVAC   CONTROL = XCF
IST1314I TRLE = TRL2B  STATUS = ACTIVE  CONTROL = XCF
IST1454I 2 TRLE(S) DISPLAYED
IST314I END
```

Displaying two TRL major nodes:

```
d net,trl,trlmn=(trl1,trl2)
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = TRL
IST1954I TRL MAJOR NODE = TRL1
IST1314I TRLE = TRL1A  STATUS = ACTIVE  CONTROL = MPC
IST1314I TRLE = TRL1B  STATUS = NEVAC   CONTROL = MPC
IST1454I 2 TRLE(S) DISPLAYED
IST924I -------------------------------------------
IST1954I TRL MAJOR NODE = TRL2
IST1314I TRLE = TRL2A  STATUS = NEVAC   CONTROL = XCF
IST1314I TRLE = TRL2B  STATUS = ACTIVE  CONTROL = XCF
IST1454I 2 TRLE(S) DISPLAYED
IST314I END
```

Displaying an active TRL entry:

```
d net,trl,trle=trle1a
IST097I DISPLAY ACCEPTED
IST075I NAME = TOC01N, TYPE = TRLE
IST1954I TRL MAJOR NODE = TRL1
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = MPC , HPDT = YES
IST1715I MPCLEVEL = HPDT       MPCUSAGE = SHARE
IST1717I ULPID = AHHCPU7 ULP INTERFACE = *NA*
IST1577I HEADER SIZE = 4092 DATA SIZE = 60 STORAGE = ***NA***
IST1221I WRITE DEV = 0CE6 STATUS = ACTIVE     STATE = ONLINE
IST1221I WRITE DEV = 0CE7 STATUS = ACTIVE     STATE = ONLINE
IST1221I WRITE DEV = 0CE8 STATUS = ACTIVE     STATE = ONLINE
IST1221I WRITE DEV = 0CE9 STATUS = ACTIVE     STATE = ONLINE
IST1577I HEADER SIZE = 4092 DATA SIZE = 60 STORAGE = DATASPACE
IST1221I READ  DEV = 0CC6 STATUS = ACTIVE     STATE = ONLINE
IST1221I READ  DEV = 0CC7 STATUS = ACTIVE     STATE = ONLINE
IST1221I READ  DEV = 0CC8 STATUS = ACTIVE     STATE = ONLINE
IST314I END
```

Displaying an active XCF TRL entry:

```
d net,trl,trle=istt1q2q
IST097I DISPLAY ACCEPTED
IST075I NAME = ISTT1Q2Q, TYPE = TRLE
IST1954I TRL MAJOR NODE = ISTTRL
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = XCF , HPDT = *NA*
IST1715I MPCLEVEL = HPDT       MPCUSAGE = SHARE
IST1717I ULPID = ISTP1Q2Q ULP INTERFACE = *NA*
IST1503I XCF TOKEN = 02000002001B0002     STATUS = ACTIVE
IST1502I ADJACENT CP = NETA.SSCP2A
IST314I END
```

Displaying an active TCP TRL entry:

```
d net,trl,trle=iutx0d20
IST097I DISPLAY ACCEPTED
IST075I NAME = IUTX0D20, TYPE = TRLE
IST1954I TRL MAJOR NODE = ISTTRL
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = TCP , HPDT = *NA*
```

```
IST1717I ULPID = TCPCS2 ULP INTERFACE = *NA*
IST1221I READ  DEV = 0D20 STATUS = ACTIVE     STATE = N/A
IST1221I WRITE DEV = 0D21 STATUS = ACTIVE     STATE = N/A
IST314I END
```

Displaying an inactive TRL entry:

```
d net,trl,trle=trle1c
IST097I DISPLAY ACCEPTED
IST075I NAME = TRLE1C, TYPE = TRLE
IST1954I TRL MAJOR NODE = TRL1
IST486I STATUS= NEVAC, DESIRED STATE= INACT
IST087I TYPE = LEASED             , CONTROL = MPC , HPDT = *NA*
IST1715I MPCLEVEL = NOHPDT     MPCUSAGE = ***N/A***
IST1221I WRITE DEV = 0508 STATUS = RESET      STATE = N/A
IST1221I WRITE DEV = 03F0 STATUS = RESET      STATE = N/A
IST1221I READ  DEV = 0408 STATUS = RESET      STATE = N/A
IST1221I READ  DEV = 02F0 STATUS = RESET      STATE = N/A
IST314I END
```

Displaying an active OSA Express TRL entry:

```
d net,trl,trle=qdio101
IST097I DISPLAY ACCEPTED
IST075I NAME = QDIO101, TYPE = TRLE
IST1954I TRL MAJOR NODE = TRLCS
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = MPC , HPDT = YES
IST1715I MPCLEVEL = QDIO       MPCUSAGE = SHARE
IST2263I PORTNAME = QDIO4101   PORTNUM =   0   OSA CODE LEVEL = ABCD
IST2337I CHPID TYPE = OSD  CHPID = C1 PNETID = NETWORK3
IST2184I QDIOSYNC = ALLINOUT - SYNCID = QDIO101 - SAVED = NO
IST1577I HEADER SIZE = 4096 DATA SIZE = 0 STORAGE = ***NA***
IST1221I WRITE DEV = 0E29 STATUS = ACTIVE     STATE = ONLINE
IST1577I HEADER SIZE = 4092 DATA SIZE = 0 STORAGE = ***NA***
IST1221I READ  DEV = 0E28 STATUS = ACTIVE     STATE = ONLINE
IST924I -------------------------------------------------------------
IST1221I DATA  DEV = 0E2A STATUS = ACTIVE     STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1717I ULPID = TCPCS1 ULP INTERFACE = QDIO4101I
IST2310I ACCELERATED ROUTING DISABLED
IST2331I QUEUE   QUEUE     READ             QUEUE
IST2332I ID      TYPE      STORAGE          STATUS
IST2205I ------  --------  ---------------  ----------------------
IST2333I RD/1    PRIMARY   4.0M(64 SBALS)   ACTIVE
IST2333I RD/2    BULKDATA  4.0M(64 SBALS)   ACTIVE
IST2333I RD/3    SYSDIST   4.0M(64 SBALS)   ACTIVE
IST2333I RD/4    EE        4.0M(64 SBALS)   ACTIVE
IST2331I QUEUE   QUEUE     READ
IST2332I ID      TYPE      STORAGE
IST2205I ------  --------  ---------------
IST2333I RD/1    PRIMARY   1.0M(16 SBALS)
IST2333I RD/2    SYSDIST   1.0M(16 SBALS)
IST2305I NUMBER OF DISCARDED INBOUND READ BUFFERS = 0
IST1757I PRIORITY1: UNCONGESTED PRIORITY2: UNCONGESTED
IST1757I PRIORITY3: UNCONGESTED PRIORITY4: UNCONGESTED
IST2190I DEVICEID PARAMETER FOR OSAENTA TRACE COMMAND = 00-05-00-00
IST1801I UNITS OF WORK FOR NCB AT ADDRESS X'15AD0010'
IST1802I P1 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P2 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P3 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P4 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST924I -------------------------------------------------------------
IST1221I TRACE DEV = 0E2B STATUS = ACTIVE     STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1717I ULPID = TCPCS1 ULP INTERFACE = QDIO6101I
IST2310I ACCELERATED ROUTING DISABLED
IST2331I QUEUE   QUEUE     READ             QUEUE
```

```
IST2332I ID      TYPE      STORAGE          STATUS
IST2205I ------  --------  ---------------  ----------------------
IST2333I RD/1    PRIMARY   4.0M(64 SBALS)   ACTIVE
IST2331I QUEUE   QUEUE     READ
IST2332I ID      TYPE      STORAGE
IST2205I ------  --------  ---------------
IST2333I RD/1    PRIMARY   4.0M(64 SBALS)
IST2305I NUMBER OF DISCARDED INBOUND READ BUFFERS = 0
IST1757I PRIORITY1: UNCONGESTED PRIORITY2: UNCONGESTED
IST1757I PRIORITY3: UNCONGESTED PRIORITY4: UNCONGESTED
IST1801I UNITS OF WORK FOR NCB AT ADDRESS X'15A92010'
IST1802I P1 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P2 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P3 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P4 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST924I -------------------------------------------------------------
IST1221I DATA  DEV = 0E2C STATUS = RESET      STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST314I END
```

Displaying a TRLE dynamically created for HiperSockets:

```
d net,trl,trle=iutiqdio
IST097I DISPLAY ACCEPTED
IST075I NAME = IUTIQDIO, TYPE = TRLE
IST1954I TRL MAJOR NODE = ISTTRL
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = MPC , HPDT = YES
IST1715I MPCLEVEL = QDIO       MPCUSAGE = SHARE
IST1716I PORTNAME = IUTIQDFE   LINKNUM =   0   OSA CODE LEVEL = *NA*
IST2337I CHPID TYPE = IQD      CHPID = FE   PNETID = ZOSNET
IST2319I IQD NETWORK ID = 07B1
IST1577I HEADER SIZE = 4096 DATA SIZE = 16384 STORAGE = ***NA***
IST1221I WRITE DEV = 0E01 STATUS = ACTIVE     STATE = ONLINE
IST1577I HEADER SIZE = 4092 DATA SIZE = 0 STORAGE = ***NA***
IST1221I READ  DEV = 0E00 STATUS = ACTIVE     STATE = ONLINE
IST924I -------------------------------------------------------------
IST1221I DATA  DEV = 0E02 STATUS = ACTIVE     STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1717I ULPID = TCPCS1 ULP INTERFACE = IUTIQDIO
IST2310I ACCELERATED ROUTING DISABLED
IST2331I QUEUE   QUEUE     READ
IST2332I ID      TYPE      STORAGE
IST2205I ------  --------  ---------------
IST2333I RD/1    PRIMARY   2.0M(126 SBALS)
IST2331I QUEUE   QUEUE     READ             QUEUE
IST2332I ID      TYPE      STORAGE          STATUS
IST2205I ------  --------  ---------------  ----------------------
IST2333I RD/1    PRIMARY   2.0M(126 SBALS)  ACTIVE
IST2305I NUMBER OF DISCARDED INBOUND READ BUFFERS = 0
IST1757I PRIORITY1: UNCONGESTED PRIORITY2: UNCONGESTED
IST1757I PRIORITY3: UNCONGESTED PRIORITY4: UNCONGESTED
IST1801I UNITS OF WORK FOR NCB AT ADDRESS X'15B18010'
IST1802I P1 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P2 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P3 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P4 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST924I -------------------------------------------------------------
IST1221I DATA  DEV = 0E03 STATUS = RESET      STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST924I -------------------------------------------------------------
IST314I END
```

Displaying an internal shared memory (ISM) TRL entry:

```
d net,trl,trle=iut00011
IST097I DISPLAY ACCEPTED
IST075I NAME = IUT00011, TYPE = TRLE
```

```
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = *NA*               , CONTROL = ISM, HPDT = *NA*
IST1954I TRL MAJOR NODE = ISTTRL
IST2418I SMCD PFID = 0011  VCHID = 0140  PNETID = ZOSNET
IST2417I VFN = 0001
IST924I -------------------------------------------------------------
IST1717I ULPID = TCPIP2 ULP INTERFACE = EZAISM02
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1500I STATE TRACE = OFF
IST314I END
```

Displaying a 10GbE RoCE Express TRLE in a dedicated RoCE environment:

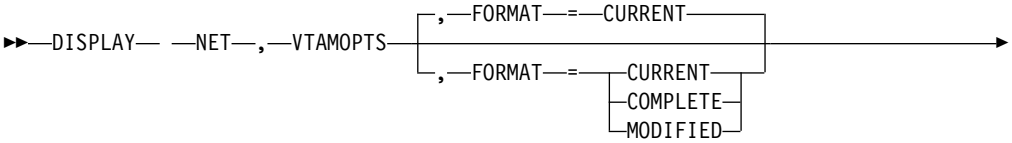
```
d net,trl,trle=iut10005
IST097I DISPLAY ACCEPTED
IST075I NAME = IUT10005, TYPE = TRLE
IST1954I TRL MAJOR NODE = ISTTRL
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = *NA*               , CONTROL = ROCE, HPDT = *NA*
IST2361I SMCR PFID = 0005  PCHID = 0500  PNETID = NETWORK3
IST2362I PORTNUM = 1  RNIC CODE LEVEL = 2.11.1200
IST2389I PFIP = 01000300
IST924I -----------------------------------------------------
IST1717I ULPID = TCPIP1 ULP INTERFACE = EZARIUT10005
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1866I TRLE = IUT10005   INOPDUMP = ON
IST924I -----------------------------------------------------
IST1717I ULPID = TCPIP2 ULP INTERFACE = EZARIUT10005
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1866I TRLE = IUT10005   INOPDUMP = ON
IST314I END
```

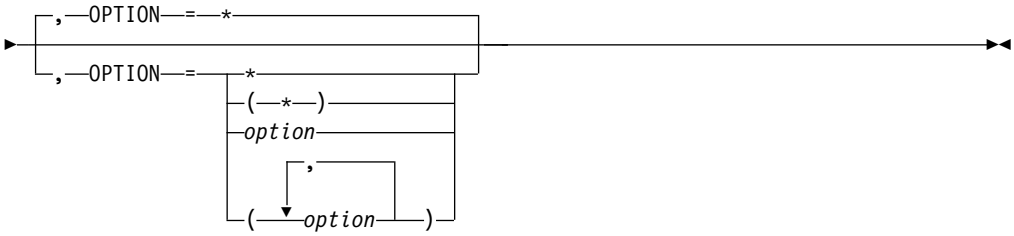
Displaying a 10GbE RoCE Express TRLE in a shared RoCE environment:

```
d net,trl,trle=iut10011
IST097I DISPLAY ACCEPTED
IST075I NAME = IUT10011, TYPE = TRLE
IST1954I TRL MAJOR NODE = ISTTRL
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = *NA*               , CONTROL = ROCE, HPDT = *NA*
IST2361I SMCR PFID = 0011  PCHID = 0140  PNETID = PNETID1
IST2362I PORTNUM = 1  RNIC CODE LEVEL = **NA**
IST2389I PFIP = 01000300
IST2417I VFN = 0001
IST924I -------------------------------------------------------------
IST1717I ULPID = TCPIP2 ULP INTERFACE = EZARIUT10011
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST314I END
```

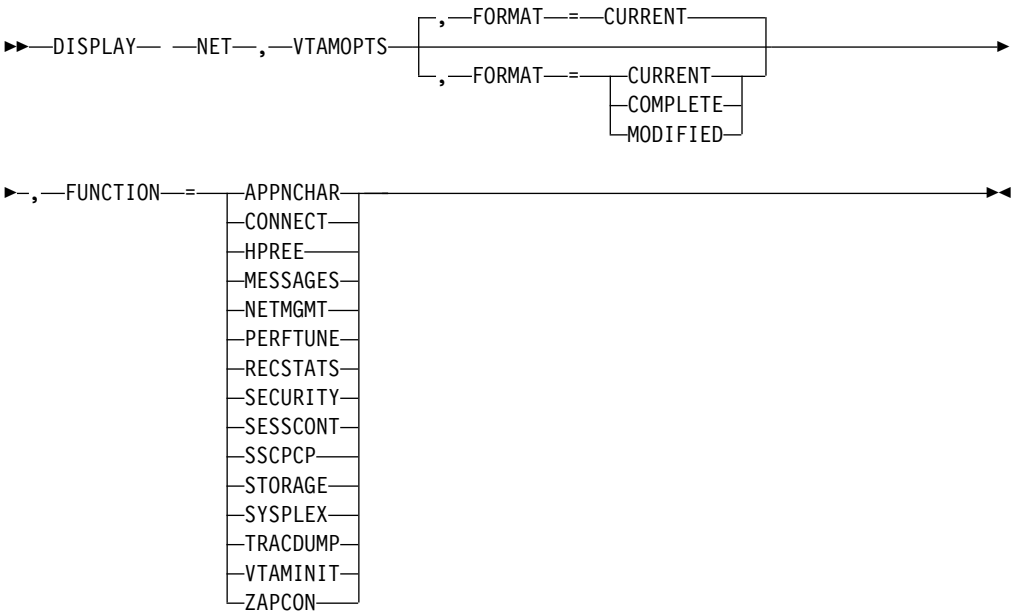
DISPLAY VTAMOPTS command

Display selected start options:





Display a group of related start options:



Abbreviations

Operand	Abbreviation
DISPLAY	D
FORMAT=COMPLETE	COMP
FORMAT=CURRENT	CUR
FORMAT=MODIFIED	MOD
OPTION	OPT

When using an abbreviation in place of an operand, code the abbreviation exactly as shown in the table. For example, when coding the abbreviation for FORMAT=CURRENT, code only CUR. Do not code FORMAT=CUR.

Purpose

The DISPLAY VTAMOPTS (VTAM start options) command displays information about VTAM start options. The VTAM version and release, the date and time when VTAM was started, the component ID, and VTAM's node type are also displayed.

Operands

FORMAT

Specifies the type of information to be displayed.

FORMAT=CURRENT

Displays the current value of one or more start options.

FORMAT=COMPLETE

Displays detailed information about one or more start options. For each start option, VTAM displays the current value, the value that VTAM initialized with, and the source of the value that VTAM initialized with. The source can be a value specified in an ATCSTRxx start option list, a value entered by the operator during VTAM start, or a default value used in the absence of any other specification.

FORMAT=MODIFIED

Displays information about start options that have been modified since VTAM initialization. If an option has not been modified, it is not displayed.

For each modified start option, VTAM displays the current value, the value that VTAM initialized with, and the source of the value that VTAM initialized with. The source can be a value specified in an ATCSTRxx start option list, a value entered by the operator during VTAM start, or a default value used in the absence of any other specification.

FUNCTION

Specifies a group of related start options to display. If you specify FUNCTION, do not specify OPTION on the same command.

FUNCTION=APPNCHAR

Displays the start options that define APPN characteristics. The start options displayed using FUNCTION=APPNCHAR are also displayed using other specifications for FUNCTION. The start options displayed using FUNCTION=APPNCHAR are:

APPNCOS	BN	BNDYN
BNORD	CDSERVR	CDSREFER
CONNTYPE	CPCP	DIRSIZE
DIRTIME	DLURSAW	DUPDEFS
DYNADJCP	EEHPRANR	EEPORTCK
EEVERIFY	GVBKDLY	HOSTNAME
HPR	HPRARB	HPRCLKRT
HPRNCPBF	HPRPSDLY	HPRPST
HPRSESLM	HPRSTALL	INITDB
IOPURGE	IPADDR	MAXLOCAT
MULTPATH	NETID	NNSPREF
NODETYPE	NUMTREES	PMTUD
PSRETRY	PSWEIGHT	RESUSAGE
ROUTERES	SACONNS	SAVERSCV
SECLVLCP	SNVC	SORDER
SRCHRED	SRCOUNT	SRTIMER
SSCPNAME	SSEARCH	TCPNAME
TDUDIAG	TOPOTIME	UNRCHTIM
VERIFYCP	VFYRED	VFYREDTI
VRTG	VRTGCPCP	XCFINIT

FUNCTION=CONNECT

Displays the start options that affect connectivity. The start options displayed using FUNCTION=CONNECT are:

AIMON	ALSREQ	AUTHLEN
CONNTYPE	CPCP	DISCNTIM
DYNHPPFX	DYNPUPFX	DYNVNPFX
ENSEMBLE	HPR	HPRNCPBF
IQDCHPID	MPCACT	NNSPREF
SACONNS	SLOWVAL	SNVC
SSDTMOUT	VRTG	VRTGCPCP
XCFGRPID	XCFINIT	XNETALS

FUNCTION=HPREE

Displays the start options that affect High Performance Routing (HPR) and Enterprise Extender (EE). The start options displayed using FUNCTION=HPREE are also displayed using other specifications for FUNCTION. The following start options are displayed using FUNCTION=HPREE:

DYNHPPFX	EEHPRANR	EEPORTCK
EEVERIFY	GVBKDLY	HOSTNAME
HPR	HPRARB	HPRCLKRT
HPRITMSG	HPRNCPBF	HPRPSDLY
HPRPSMSG	HPRPST	HPRSESLM
HPRSTALL	IPADDR	MAXEETST
MAXHNRES	MULTPATH	PMTUD
PSRETRY	PSWEIGHT	TCPNAME
UNRCHTIM		

FUNCTION=MESSAGES

Displays the start options that affect messages. The start options displayed using FUNCTION=MESSAGES are:

ASIRFMSG	CNMTAB	CNNRTMSG
DSIRFMSG	DSPLYDEF	DSPLYMAX
DSPLYWLD	ESIRFMSG	FLDTAB
FSIRFMSG	HPRITMSG	HPRPSMSG
IOINT	IOMSGLIM	LSIRFMSG
MSGLEVEL	MSGMOD	PLUALMSG
PPOLOG	RSIRFMSG	SIRFMSG
SLOWVAL	VARYWLD	

FUNCTION=NETMGMT

Displays the start options that affect network management. The start options displayed using FUNCTION=NETMGMT are also displayed using other specifications for FUNCTION. The following start options are displayed using FUNCTION=NETMGMT:

CNMTAB	DLURSAW	IPINFO
MXSAWBUF	NMVTLOG	OSIEVENT
OSIMGMT	OSITOPO	PDTRCBUF
SAWMAXDS	SAWMXQPK	SNAMGMT
UPDDELAY		

FUNCTION=PERFTUNE
Displays the start options that affect performance and tuning. The start options displayed using FUNCTION=PERFTUNE are:

AUTOTI	BSCTMOUT	CACHETI
CDRSCTI	CINDXSIZ	DIRSIZE
DIRTIME	HNTSIZE	HPRARB
HPRCLKRT	HPRITMSG	HPRPSDLY
HPRPSMSG	HPRPST	HPRSESLM
HSRTSIZE	IOINT	IOPURGE
IQDIOSTG	MAXEETST	MAXHNRES
MAXLOCAT	MAXLURU	MIHTMOUT
MULTPATH	MXSAWBUF	MXSSCPRU
NCPBUFSZ	NSRTSIZE	NUMTREES
OSIEVENT	OSITOPO	OSRTSIZE
PDTRCBUF	PIUMAXDS	PMTUD
PSRETRY	PSWEIGHT	QDIOSTG
SAWMAXDS	SAWMXQPK	SONLIM
SRCHRED	SRCOUNT	SRTIMER
UPDDELAY	VFYRED	VFYREDTI
VOSDEACT	VTAMEAS	

FUNCTION=RECSTATS
Displays the start options that affect recording and statistics. The start options displayed using FUNCTION=RECSTATS are:

BSCMDRS	NMVTLOG	PPOLOG
SDLCMDRS	TNSTAT	

FUNCTION=SECURITY
Displays the start options that affect session security. The start options displayed using FUNCTION=SECURITY are:

ENCRPREF	ENCRYPTN	IPINFO
SECLVLCP	VERIFYCP	

FUNCTION=SESSCONT
Displays the start options that affect session control. The start options displayed using FUNCTION=SESSCONT are:

AFFDELAY	APPNCOS	ASYDE
AUTORTRY	BNDYN	BNORD
CDRDYN	CMPMIPS	CMPVTAM
CPCDRSC	DIALRTRY	DLRORDER
DUPDEFS	DYNADJCP	DYNASSCP
DYNDLGMD	DYNLU	DYNMODTB
EXPFLTRM	HOTIOTRM	HPRSESLM
ISTCOSDF	RESUSAGE	ROUTERES
SMEAUTH	SORDER	SSCPDYN
SSCPORD	SSEARCH	SWNORDER
UNRCHTIM		

FUNCTION=SSCPCP
Displays the start options that define SSCP or CP characteristics. The start options displayed using FUNCTION=SSCPCP are:

BN	CDSERVR	DATEFORM
ENHADDR	GWSSCP	HOSTPU
HOSTSA	LIMINTCP	MAINTLVL
MAXSSCPS	MAXSUBA	MXSUBNUM
NETID	NNSPREF	NODETYPE
NQNMODE	SSCPID	SSCPNAME
STRGR	STRMNPS	TRANSLAT
USSTAB		

FUNCTION=STORAGE
Displays the start options that define storage usage, except for the buffer pool start options. The start options displayed using FUNCTION=STORAGE are:

API64R	CSALIMIT	CSA24
DLRTCB	IRNSTRGE	MAXHNRES
VTAMEAS		

FUNCTION=SYSPLEX
Displays the start options that affect coupling facility and the sysplex. The start options displayed using FUNCTION=SYSPLEX are also displayed using other specifications for FUNCTION. The following start options are displayed using FUNCTION=SYSPLEX:

AFFDELAY	STRGR	STRMNPS
XCFGRPID	XCFINIT	

FUNCTION=TRACDUMP
Displays the start options that affect traces and dumps. The start options displayed using FUNCTION=TRACDUMP are:

INOPDUMP	NACPROBE	PSSTRACE	SNAPREQ

FUNCTION=VTAMINIT
Displays the start options that affect VTAM initialization. The start options displayed using FUNCTION=VTAMINIT are:

COLD	CONFIG	INITDB
LIST	NODELST	OSIMGMT
SNAMGMT	WARM	

FUNCTION=ZAPCON
Displays the start options that once were zappable constants. The start options displayed using FUNCTION=ZAPCON are also displayed using other specifications for FUNCTION. The start options displayed using FUNCTION=ZAPCON are:

ASIRFMSG	BSCTMOUT	CINDXSIZ
ESIRFMSG	FSIRFMSG	HNTSIZE
HSRTSIZE	INOPDUMP	IOMSGLIM
IRNSTRGE	MAXLURU	MAXSSCPS
MIHTMOUT	MXSAWBUF	MXSSCPRU
MXSUBNUM	NCPBUFSZ	OSRTSIZE
PDTRCBUF	PIUMAXDS	PLUALMSG
PSSTRACE	SAWMAXDS	SAWMXQPK

SDLCMDRS SIRFMSG SLUALMSG
SNAPREQ SSDTMOUT TRANSLAT
VTAMEAS

OPTION=option
Specifies one or more start options to display. If you specify OPTION, do not specify FUNCTION on the same command. If OPTION=* is specified or assumed by default, VTAM displays information about all start options except INOPCODE, PROMPT, NOPROMPT, LISTBKUP, and the trace and buffer pool start options. The DISPLAY INOPCODE command can be used to display the current dump attributes. The DISPLAY TRACES command and the DISPLAY BFRUSE command can be used to display trace and buffer pool information. See the z/OS Communications Server: SNA Resource Definition Reference for a description of each start option.

For OPTION=LIST, VTAM displays the name of the start option list used during start processing. The value can be a supplemental list, such as LIST=1A. However, if the supplemental list contains errors and VTAM reverts to using defaults during start processing because LISTBKUP=DEFAULTS is in effect, the user-defined default list will be displayed. You can also issue a D NET,VTAMOPTS,FORMAT=COMPLETE command to find out the origin of the start option values.

For OPTION=CNMTAB, VTAM displays *BLANKS* if a user-defined table was not loaded. You can issue a D NET,VTAMOPTS,FORMAT=COMPLETE command to find out the origin of the start option value.

For OPTION=ENCRYPTN, the display might not exactly match the value specified for the ENCRYPTN start option.

The following list shows the values that can be displayed for ENCRYPTN for each value specified on the start option:

Start value
Display value

NO NO

YES, 24, or 31
24 or 31

CCA CCA_24 or CCA_31

CUSP CUSP_24 or CUSP_31

For OPTION=OSIMGMT, VTAM displays only the value of the OSIMGMT start option. It does not indicate whether CMIP services is active.

For OPTION=STRGR or OPTION=STRMNPS, if no coupling facility is in use, this command shows the value as ***NA***. See z/OS MVS Setting Up a Sysplex for more information about coupling facilities and CFRM.

See the z/OS Communications Server: SNA Network Implementation Guide for more information about the sources of start options and which source takes precedence.

For OPTION=INOPDUMP, the display might not match the values that are coded for the INOPDUMP start option. The following values are valid:

- ON, which represents an encoding of INOPDUMP=ON.
- OFF, which represents an encoding of INOPDUMP=OFF.
- One or more INOPDUMP control groups in the following format, where the INOPDUMP control group is listed if the current setting for the control group is INOPDUMP=ON.

  ```
  control_group1, ... ,control_group-x
  ```

Example 1

1. VTAM is started with INOPDUMP=OFF.
2. The operator issues MODIFY VTAMOPTS,INOPDUMP=(ON,ISM,ROCE).
3. A DISPLAY VTAMOPTS,OPT=INOPDUMP displays a start option value of (ISM,ROCE), because those two control groups settings are INOPDUMP=ON.

Example 2

1. VTAM is started with INOPDUMP=ON.
2. Subsequently, the operator issues MODIFY VTAMOPTS,INOPDUMP=(OFF,BASE,XCF,QDIO).
3. A DISPLAY VTAMOPTS,OPT=INOPDUMP displays a start option value of (IQDIO,ISM,ROCE,TCP), because those four control groups settings are still INOPDUMP=ON.

See z/OS Communications Server: SNA Resource Definition Reference for more information about coding the INOPDUMP start option.

Resulting display

The resulting display shows:

- The VTAM version and release
- The time and date that VTAM was started
- The component ID
- The node type
- Information about the specified start options

If a start option is not applicable to your configuration, it is displayed with ***NA***. For example, ROUTERES is applicable only when VTAM is a network node. At an end node, it would be displayed as ROUTERES=***NA***.

Examples

Displaying start options that have been modified:

```
d net,vtamopts,opt=(sscpid,dsplydef,cmpvtam,cpcp,tnstat,hostname),format=modified
IST097I DISPLAY ACCEPTED
IST1188I ACF/VTAM CSV2R10 STARTED AT 11:54:32 ON 03/23/00
IST1349I COMPONENT ID IS 5695-11701-10A
IST1348I VTAM STARTED AS INTERCHANGE NODE
IST1309I START OPTION  CURRENT VALUE     ORIGINAL VALUE    ORIGIN
IST1310I CMPVTAM       2                 0                 DEFAULT
IST1310I CPCP          NO                YES               ATCSTR1A
IST1310I DSPLYDEF      32767             65535             ATCSTR00
IST1310I TNSTAT        OFF               CNSL,TIME=1       OPERATOR
IST924I -------------------------------------------------------------
IST19051 START OPTION   = HOSTNAME
```

```
IST1906I CURRENT VALUE  = NODENAME.NETID.REALLYLONGDOMAIN.COM
IST1907I ORIGINAL VALUE = NODENAME.NETID.SHORTDOMAIN.COM
IST1908I ORIGIN         = OPERATOR
IST314I END
```

Displaying complete information about selected start options:

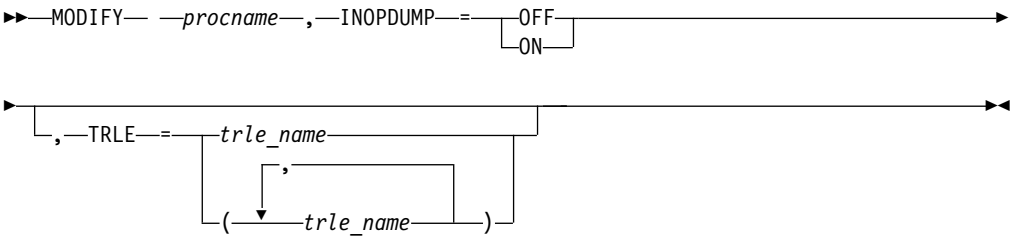
```
d net,vtamopts,opt=(dynlu,dsplydef,list,cmpvtam,supp,cpcp,tnstat,hostname),
format=complete
IST097I DISPLAY ACCEPTED
IST1188I ACF/VTAM CSV2R10 STARTED AT 11:54:32 ON 03/23/00
IST1349I COMPONENT ID IS 5695-11701-10A
IST1348I VTAM STARTED AS INTERCHANGE NODE
IST1309I START OPTION  CURRENT VALUE     ORIGINAL VALUE    ORIGIN
IST1310I CMPVTAM       2                 0                 DEFAULT
IST1310I CPCP          NO                YES               ATCSTR1A
IST1310I DSPLYDEF      32767             65535             ATCSTR00
IST1310I DYNLU         YES               YES               ATCSTR1A
IST1310I LIST          1A                1A                OPERATOR
IST1310I SUPP          NOSUP             NOSUP             ATCSTR00
IST1310I TNSTAT        OFF               CNSL,TIME=1       OPERATOR
IST924I -------------------------------------------------------------
IST1905I START OPTION   = HOSTNAME
IST1906I CURRENT VALUE  = NODENAME.NETID.REALLYLONGDOMAIN.COM
IST1907I ORIGINAL VALUE = NODENAME.NETID.SHORTDOMAIN.COM
IST1908I ORIGIN         = OPERATOR
IST314I END
```

Displaying all VTAM start options:

```
D NET,VTAMOPTS
IST097I DISPLAY ACCEPTED
IST1188I VTAM CSV2R2 STARTED AT 14:30:12 ON 05/22/15
IST1349I COMPONENT ID IS 5695-11701-220
IST1348I VTAM STARTED AS INTERCHANGE NODE
IST1189I AFFDELAY = 600                 AIMON    = NONE
IST1189I ALSREQ   = NO                  API64R   = YES
IST1189I APPNCOS  = NONE                ASIRFMSG = OLUSSCP
IST1189I ASYDE    = TERM                AUTHLEN  = YES
IST1189I AUTORTRY = AUTOCAP             AUTOTI   = 0
IST1189I BN       = NO                  BNDYN    = ***NA***
IST1189I BNORD    = ***NA***            BSCMDRS  = (STATS,INOPS)
IST1189I BSCTMOUT = 286                 CACHETI  = 8
IST1189I CDRDYN   = YES                 CDRSCTI  = 480S
IST1189I CDSERVR  = NO                  CDSREFER = 1
IST1189I CINDXSIZ = 8176                CMPMIPS  = 100
IST1189I CMPVTAM  = 0                   CNMTAB   = ISTMGC00
IST1189I CNNRTMSG = SUPPRESS            COLD     = YES
IST1189I CONFIG   = 1A                  CONNTYPE = APPN
IST1189I CPCDRSC  = NO                  CPCP     = YES
IST1189I CSALIMIT = 240163K             CSA24    = NOLIMIT
IST1189I DATEFORM = MDY                 DIALRTRY = YES
IST1189I DIRSIZE  = 0                   DIRTIME  = 691200S
IST1189I DISCNTIM = (15,0)              DLRORDER = (STATNID,FIRST)
IST1189I DLRTCB   = 5                   DLURSAW  = YES
IST1189I DSIRFMSG = NONE                DSPLYDEF = 65535
IST1189I DSPLYMAX = 65535               DSPLYWLD = FULLWILD
IST1189I DUPDEFS  = ALL                 DYNADJCP = YES
IST1189I DYNASSCP = YES                 DYNDLGMD = NONE
IST1189I DYNHPPFX = CNR                 DYNLU    = YES
IST1189I DYNMODTB = NONE                DYNPUPFX = CN
IST1189I DYNVNPFX = CNV                 EEHPRANR = NO
IST1189I EEPORTCK = NO                  EEVERIFY = ACTIVATE
IST1189I ENCRPREF = NONE                ENCRYPTN = 31
IST1189I ENHADDR  = YES                 ENSEMBLE = ***NA***
IST1189I ESIRFMSG = ALLSSCP             EXPFLTRM = 0
IST1189I FLDTAB   = ISTMSFLD            FSIRFMSG = OLUSSCP
IST1189I GVBKDLY  = NO                  GWSSCP   = YES
```

```
IST1189I HNTSIZE  = 4080                HOSTNAME = *BLANKS*
IST1189I HOSTPU   = ISTPUS              HOSTSA   = 1
IST1189I HOTIOTRM = 0                   HPR      = (RTP,RTP)
IST1189I HPRARB   = RESPMODE            HPRCLKRT = STANDARD
IST1189I HPRITMSG = BASE                HPRNCPBF = NO
IST1189I HPRPSDLY = 0                   HPRPSMSG = ALL
IST1189I HPRPST   = LOW          480S   HPRPST   = MEDIUM       240S
IST1189I HPRPST   = HIGH         120S   HPRPST   = NETWRK        60S
IST1189I HPRSESLM = NOLIMIT             HPRSTALL = 0
IST1189I HSRTSIZE = 9973                INITDB   = ALL
IST1189I INOPDUMP = OFF                 IOINT    = 180
IST1189I IOMSGLIM = 100                 IOPURGE  = 0
IST1189I IPADDR   = 0.0.0.0             IPINFO   = SENDALL
IST1189I IQDCHPID = ANY                 IQDIOSTG = 7.8M(126 SBALS)
IST1189I IRNSTRGE = 0                   ISTCOSDF = INDLU
IST1189I LIMINTCP = ***NA***            LIST     = 1A
IST1189I LSIRFMSG = NONE                MAINTLVL = *BLANKS*
IST1189I MAXEETST = 500                 MAXHNRES = 100
IST1189I MAXLOCAT = 5000                MAXLURU  = 6144
IST1189I MAXSSCPS = 10                  MAXSUBA  = 255
IST1189I MIHTMOUT = 1800                MPCACT   = WAIT
IST1189I MSGLEVEL = BASE                MSGMOD   = NO
IST1189I MULTPATH = NO                  MXSAWBUF = 10000
IST1189I MXSSCPRU = 4096                MXSUBNUM = 511
IST1189I NACPROBE = NODUMP              NCPBUFSZ = 512
IST1189I NETID    = NETA                NMVTLOG  = NPDA
IST1189I NNSPREF  = ***NA***            NODELST  = *BLANKS*
IST1189I NODETYPE = NN                  NQNMODE  = NAME
IST1189I NSRTSIZE = *BLANKS*            NUMTREES = 100
IST1189I OSIEVENT = PATTERNS            OSIMGMT  = NO
IST1189I OSITOPO  = ILUCDRSC            OSRTSIZE = 43
IST1189I PDTRCBUF = 2                   PIUMAXDS = 200
IST1189I PLUALMSG = NOSUPP              PMTUD    = TCPVALUE
IST1189I PPOLOG   = NO                  PSRETRY  = LOW             0S
IST1189I PSRETRY  = MEDIUM         0S   PSRETRY  = HIGH            0S
IST1189I PSRETRY  = NETWRK         0S   PSRETRY  = SCHED
IST1189I PSSTRACE = NORB                PSWEIGHT = LESSTHAN
IST1189I QDIOSTG  = 4.0M(64 SBALS)      RESUSAGE = 100
IST1189I ROUTERES = 1                   RSIRFMSG = ALLSSCP
IST1189I SACONNS  = YES                 SAVERSCV = (NO,KEEP)
IST1189I SAWMAXDS = 100                 SAWMXQPK = 0
IST1189I SDLCMDRS = (STATS,INOPS)       SECLVLCP = ***NA***
IST1189I SIRFMSG  = ALLSSCP             SLOWVAL  = (0,0)
IST1189I SLUALMSG = NOSUPP              SMEAUTH  = DISCARD
IST1189I SNAMGMT  = NO                  SNAPREQ  = 1000
IST1189I SNVC     = ***NA***            SONLIM   = (60,30)
IST1189I SORDER   = APPN                SRCHRED  = OFF
IST1189I SRCOUNT  = 10                  SRTIMER  = 30S
IST1189I SSCPDYN  = YES                 SSCPID   = 1
IST1189I SSCPNAME = SSCP1A              SSCPORD  = PRIORITY
IST1189I SSDTMOUT = 30                  SSEARCH  = YES
IST1189I STRGR    = ***NA***            STRMNPS  = ***NA***
IST1189I SUPP     = NOSUP               SWNORDER = (CPNAME,FIRST)
IST1189I TCPNAME  = *BLANKS*            TDUDIAG  = 1000
IST1189I TNSTAT   = OFF                 TOPOTIME = 14:30
IST1189I TRANSLAT = (0,1,2,3,4,5,6,7)   UNRCHTIM = (0,0)
IST1189I UPDDELAY = 60S                 USSTAB   = *BLANKS*
IST1189I VARYWLD  = FULLWILD            VERIFYCP = NONE
IST1189I VFYRED   = YES                 VFYREDTI = OFF
IST1189I VOSDEACT = NO                  VRTG     = NO
IST1189I VRTGCPCP = YES                 VTAMEAS  = 32001
IST1189I WARM     = NO                  XCFGRPID = ***NA***
IST1189I XCFINIT  = ***NA***            XNETALS  = NO
IST314I END
```

MODIFY INOPDUMP command



Abbreviations

Operand	Abbreviation
MODIFY	F

Purpose

INOPDUMP controls the automatic dumping of VTAM when an inoperative condition occurs in one of VTAMs data link control layers (DLCs). There are three separate but related controls:

- The global INOPDUMP status, which is also the VTAM INOPDUMP start option. The global INOPDUMP status can be set for all DLCs or it can be selectively set for a subset of resources that are associated with an INOPDUMP control group. If the global INOPDUMP status is on for all resources, or is on for the BASE control group, this controls automatic dumping when an inoperative condition is declared on a resource that is not defined within a TRLE (transport resource list entry). The global INOPDUMP status is copied to the TRLE when a TRLE is activated if the TRLE InOpDump status has not been explicitly set.
- The TRLE INOPDUMP status which controls automatic dumping when an inoperative condition is declared on a resource that is defined within the TRLE.
- The INOPCODE status, which controls whether a given code in the module detecting the inoperative condition is enabled for automatic dumping. See MODIFY INOPCODE command for more details on the interaction between INOPDUMP and INOPCODE.

Use MODIFY INOPDUMP to alter either the global or TRLE INOPDUMP status. Use the MODIFY VTAMOPTS, INOPDUMP command to alter the INOPDUMP global status selectively using control groups.

Operands

procname
The procedure name for the command. If procname in the START command was specified as startname.ident, where startname is the VTAM start procedure and ident is the optional identifier, either startname.ident or ident can be specified for procname.

If procname in the START command was startname, startname must be specified for procname.

INOPDUMP=ON
Specifies that either the global or TRLE inopdump status is to be set on for all resources.

INOPDUMP=OFF
Specifies that either the global or TRLE inopdump status is to be set off for all resources.

TRLE=trle_name
Specifies the TRLE name or names for which the INOPDUMP status is to be altered.

Note:

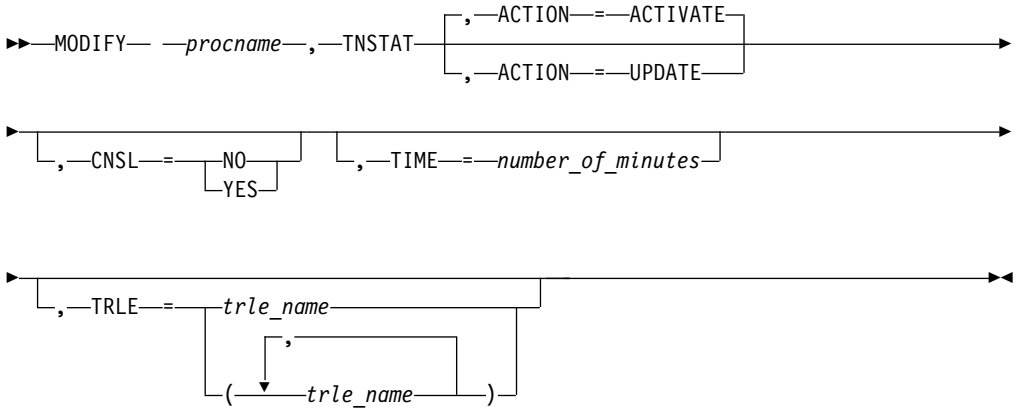
1. If the TRLE operand is not specified, both the global and TRLE statuses are altered. If the TRLE operand is specified, only the status of the TRLE for the name or names specified is altered and the global status remains unchanged.
2. The response to a successful global Modify INOPDUMP command will always include the global INOPDUMP status. If the TRL major node was available at the time of the command, you will receive a reminder message that the status for all TRLEs has also been changed. The response to a successful Modify INOPDUMP command that includes the TRLE option will always include the global INOPDUMP status along with the TRLE name or names that were processed.

Examples

Modifying INOPDUMP information:

```
f vtam,inopdump=off,trle=trle1a
   IST097I MODIFY ACCEPTED
   IST1865I GLOBAL INOPDUMP = OFF
   IST1866I TRLE = TRLE1A   INOPDUMP = OFF
   IST314I END
   IST223I MODIFY INOPDUMP COMMAND COMPLETED
```

MODIFY TNSTAT command



Abbreviations

Operand	Abbreviation
MODIFY	F
ACTION=ACTIVATE	ACTIVATE or A
ACTION=UPDATE	UPDATE or U
CNSL=NO	NOCNSL

Operand	Abbreviation
CNSL=YES	CNSL

When using an abbreviation in place of an operand, code the abbreviation exactly as shown in the table. For example, when coding the abbreviation for CNSL=YES, code only CNSL.

Purpose

VTAM can record tuning statistics about some of its activities. You can use these statistics to set the proper values on resource definition operands that control VTAM I/O operations in your system. You can use tuning statistics to gather information about the following connections:

- Channel-to-channel
- Multipath channel
- Remote Direct Memory Access (RDMA) over converged Ethernet (ROCE)
- SNA controller
- TCP

You cannot use VTAM tuning statistics to gather information about internal shared memory (ISM) devices. However, you can obtain some tuning statistics for ISM interfaces by using the Netstat DEvlinks/-d report. For more information, see Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands.

For more information about using tuning statistics, see the z/OS Communications Server: SNA Network Implementation Guide.

You can record external trace data using the system management facility (SMF) in the system during system generation.

MODIFY TNSTAT reopens the tuning statistics file if it was closed by a previous MODIFY NOTNSTAT command.

Operands

procname
The procedure name for the command. If *procname* in the START command was specified as *startname.ident*, where *startname* is the VTAM start procedure and *ident* is the optional identifier, either *startname.ident* or *ident* can be specified for *procname*.

If *procname* in the START command was *startname*, *startname* must be specified for *procname*.

ACTION=ACTIVATE
Specifies the TNSTAT recording is to be initiated.

ACTION=UPDATE
Specifies either or both the CNSL and TIME operands are to be processed without initiating recording.

CNSL
Specifies whether tuning statistics are to be sent to the system console.

The CNSL operand is placed in effect for all devices collecting tuning statistics.

CNSL=YES
Specifies that tuning statistics records are to be sent to the system console.

CNSL=NO
Specifies that tuning statistics records are not to be sent to the system console.

TIME=number_of_minutes
Specifies the number of minutes in the tuning statistics reporting interval. At the end of each interval, summary records are sent to SMF (if SMF is active) and to the system console (if CNSL=YES). Specify this number as a decimal integer in the range 1–1440. If the TIME operand is not specified, the following situations will occur:

- If this is the first activation of tuning statistics a default of 60 minutes is used.
- If tuning statistics was previously activated then deactivated, the value that was in effect when tuning statistics was deactivated is reinstated.

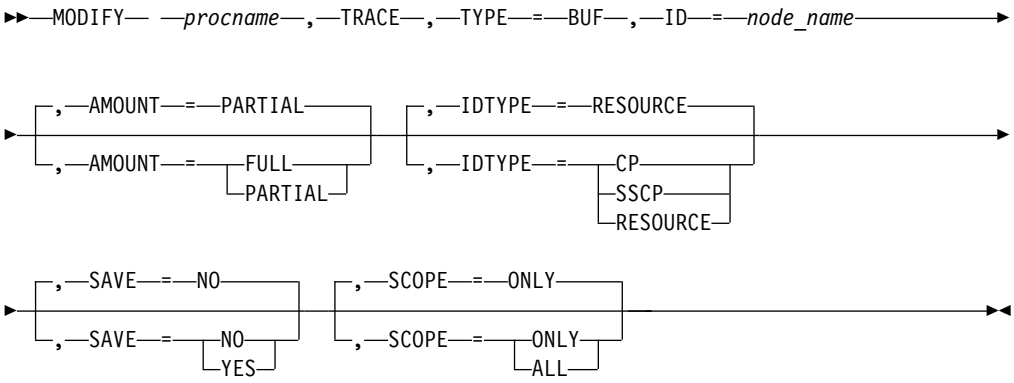
TRLE=*trle_name*
Specifies the Transport Resource List Entry name or names for which statistical recording is to be initiated.

Note: Recording is initiated only for those devices within the specified TRLE or TRLEs. If the TRLE operand is not specified, recording is initiated for all devices that collect tuning statistics.

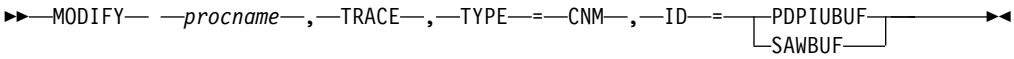
The TRLE operand is mutually exclusive with the ACTION=UPDATE operand.

MODIFY TRACE command

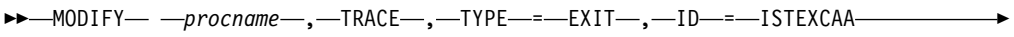
Start or modify a buffer contents trace:

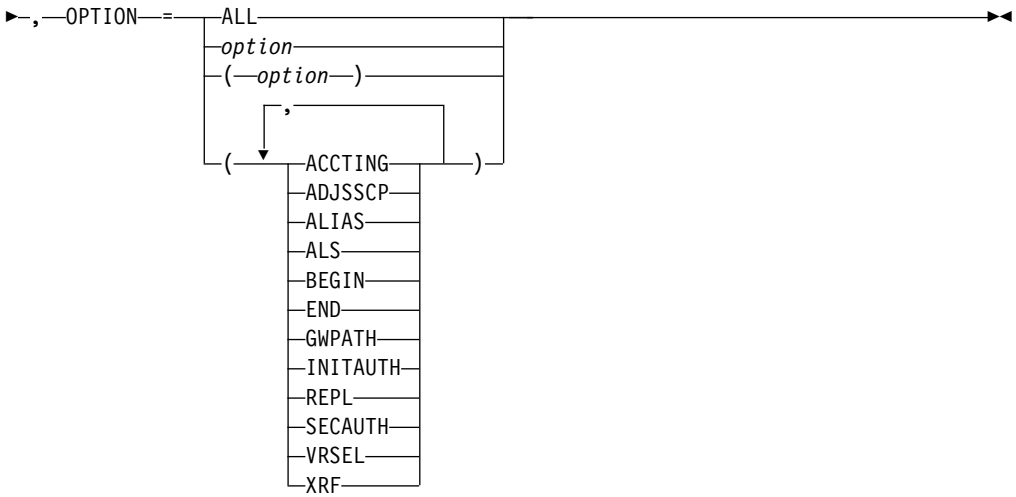


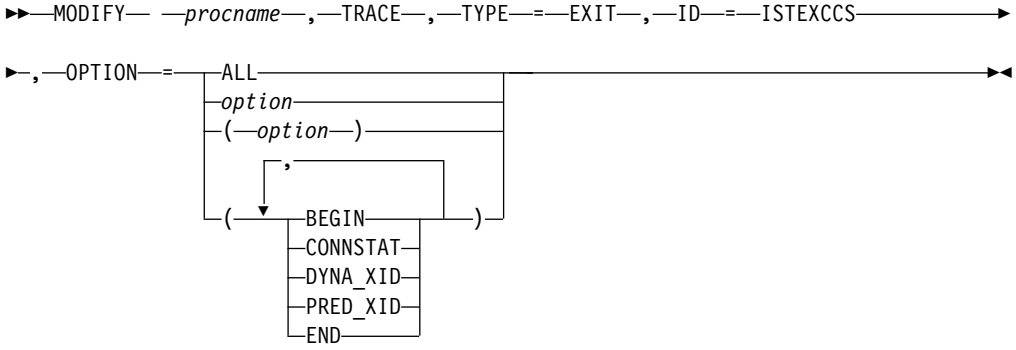
Start or modify a communication network management trace:

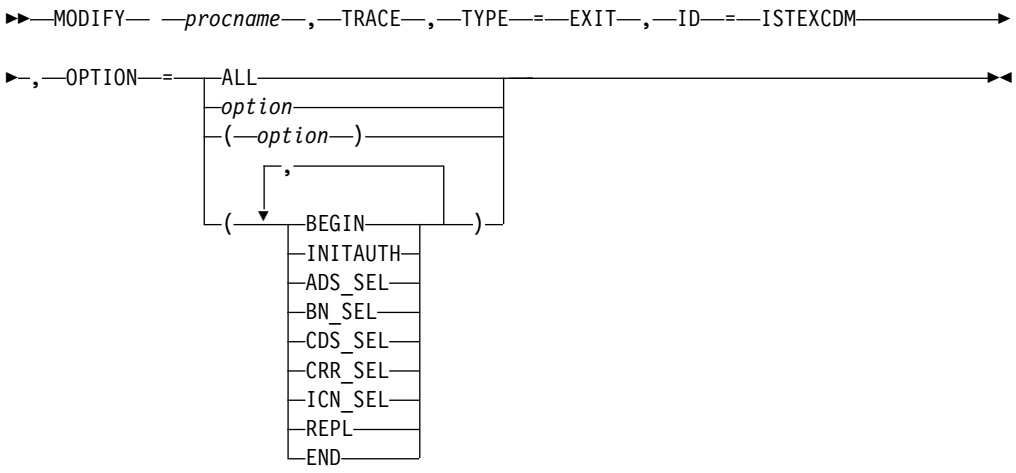


Start or modify a user Exit buffer trace:

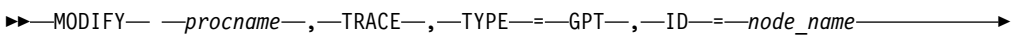


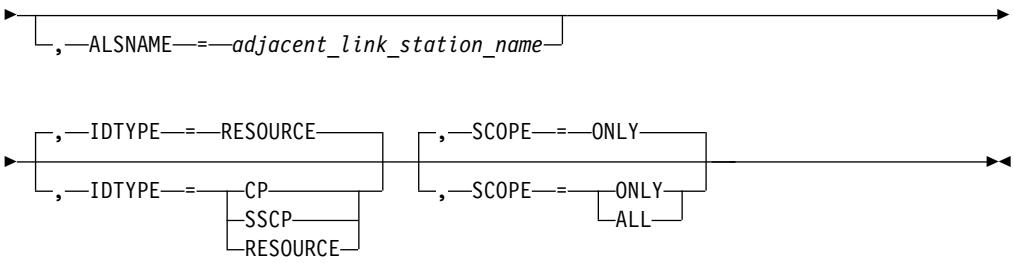




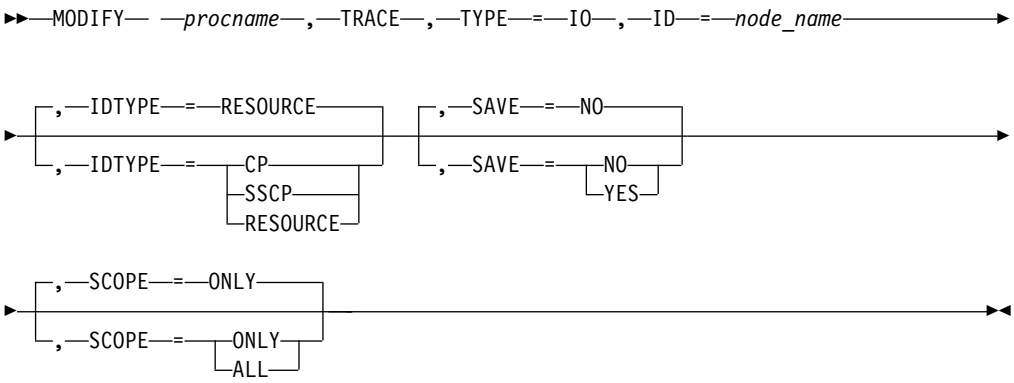


Start or modify a generalized PIU trace:

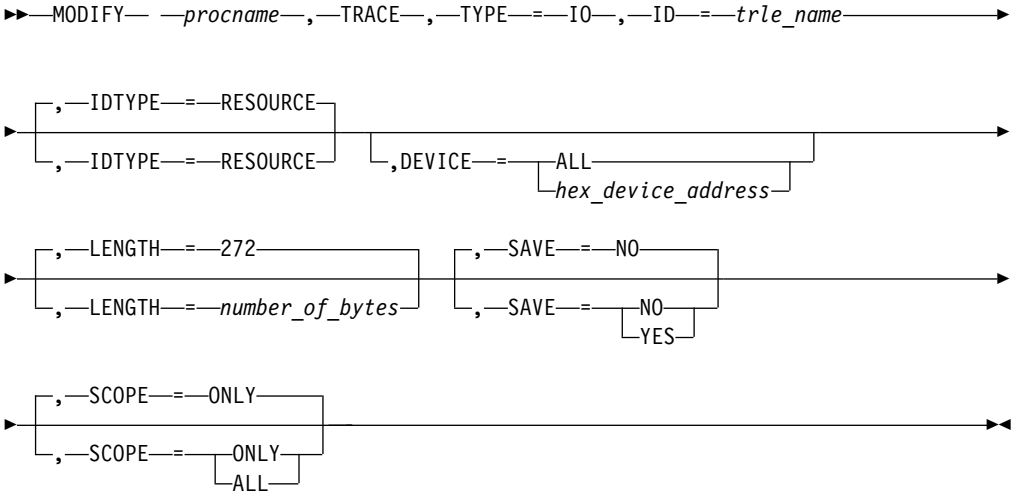




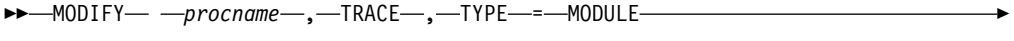
Start or modify an input/output trace:

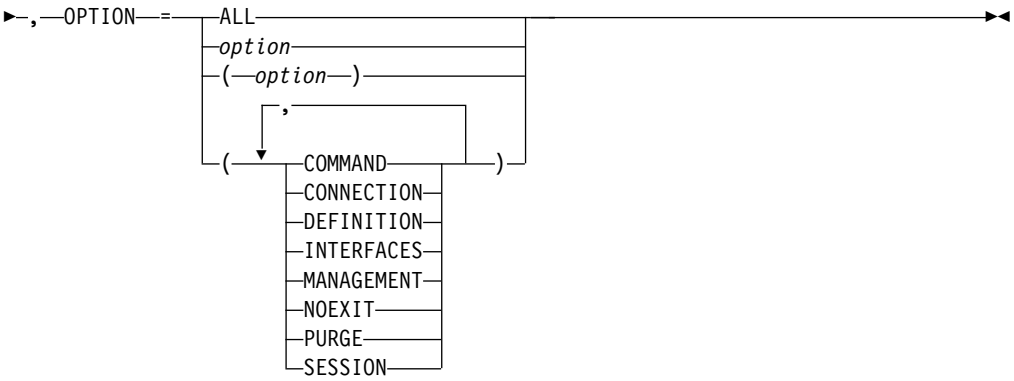


Start or modify an input/output trace for a TRLE with the DATAPATH operand coded:

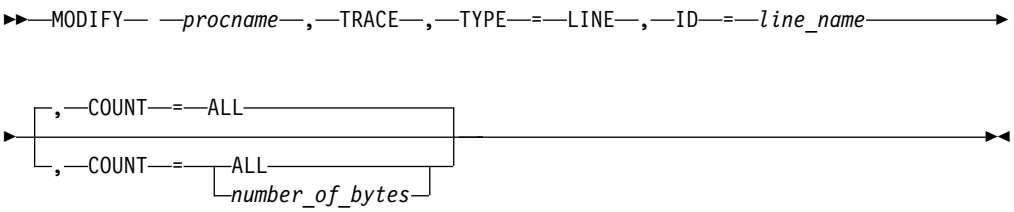


Start or modify a module trace:

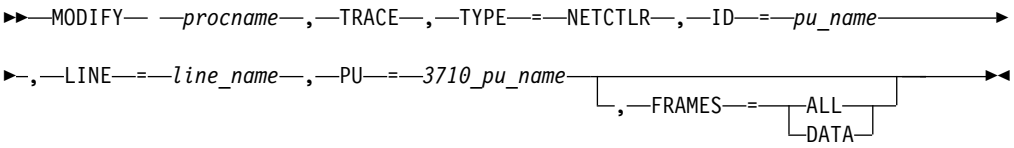




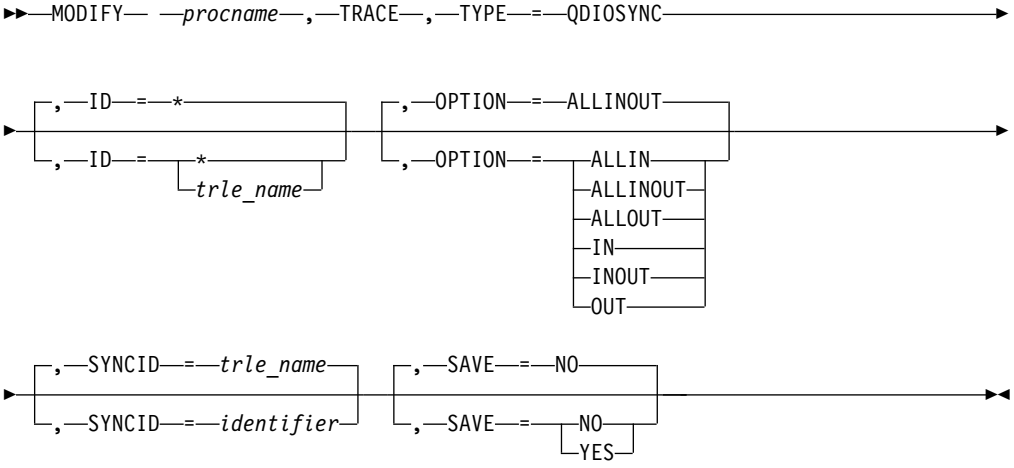
Start or modify an NCP line trace:



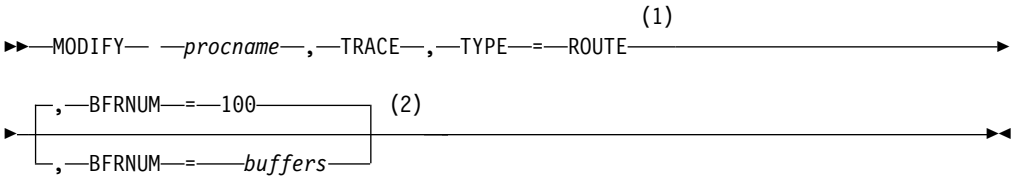
Start or modify a 3710 Network Controller line trace:



Start or modify OSA-Express2 diagnostic data synchronization for an OSA-Express2 adapter:



Start the APPN route selection trace in a network node:

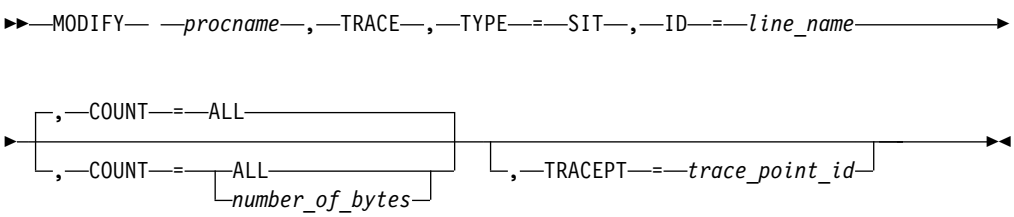


Notes:

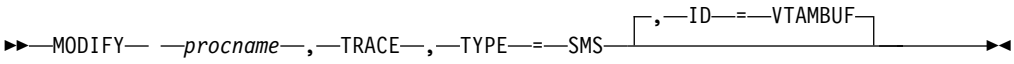
1 TYPE=ROUTE is allowed only in a network node.

2 The initial default value for BFRNUM is 100. When the initial value has been set, it remains until the value is changed with BFRNUM specified on another MODIFY TRACE command.

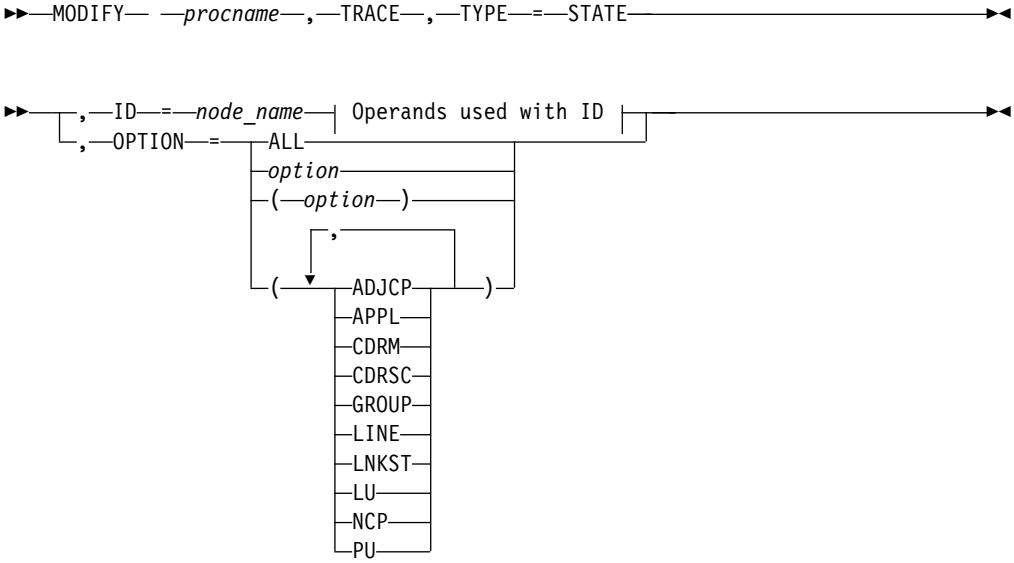
Start or modify a scanner interface trace:



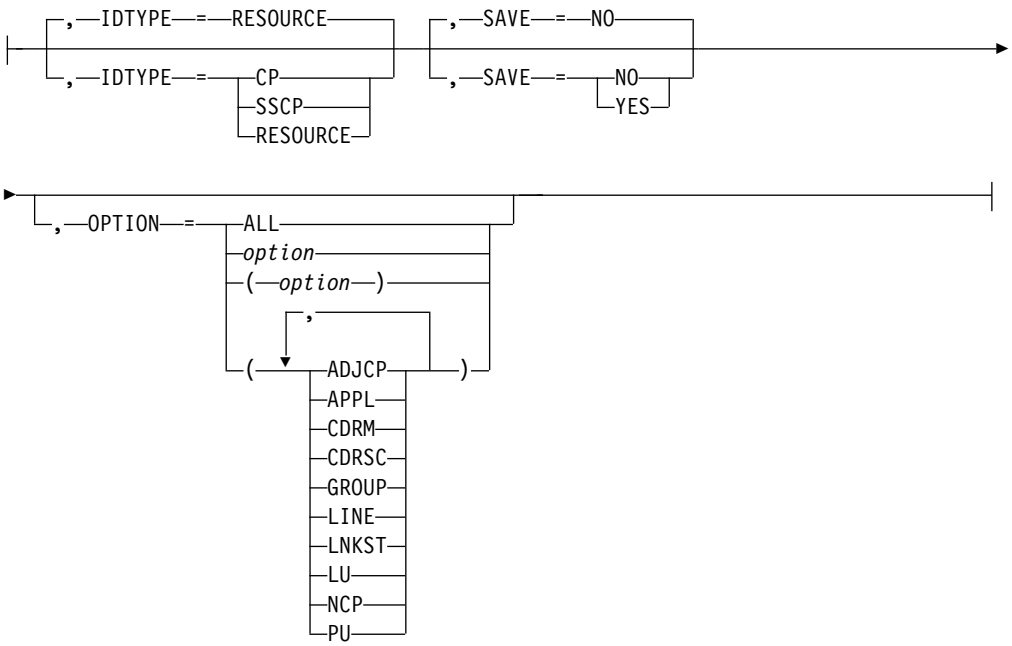
Start or modify an SMS (buffer use) trace:



Start or modify a resource state trace:



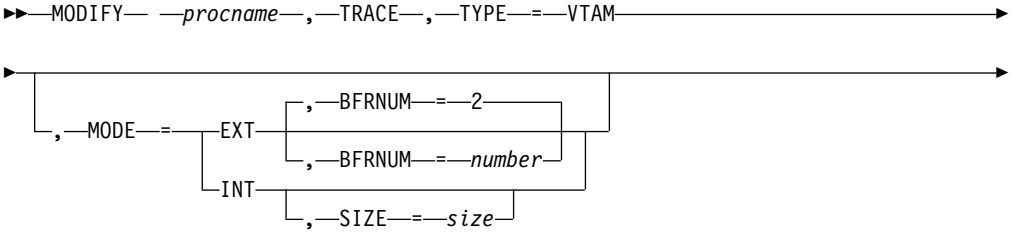
Operands used with ID:

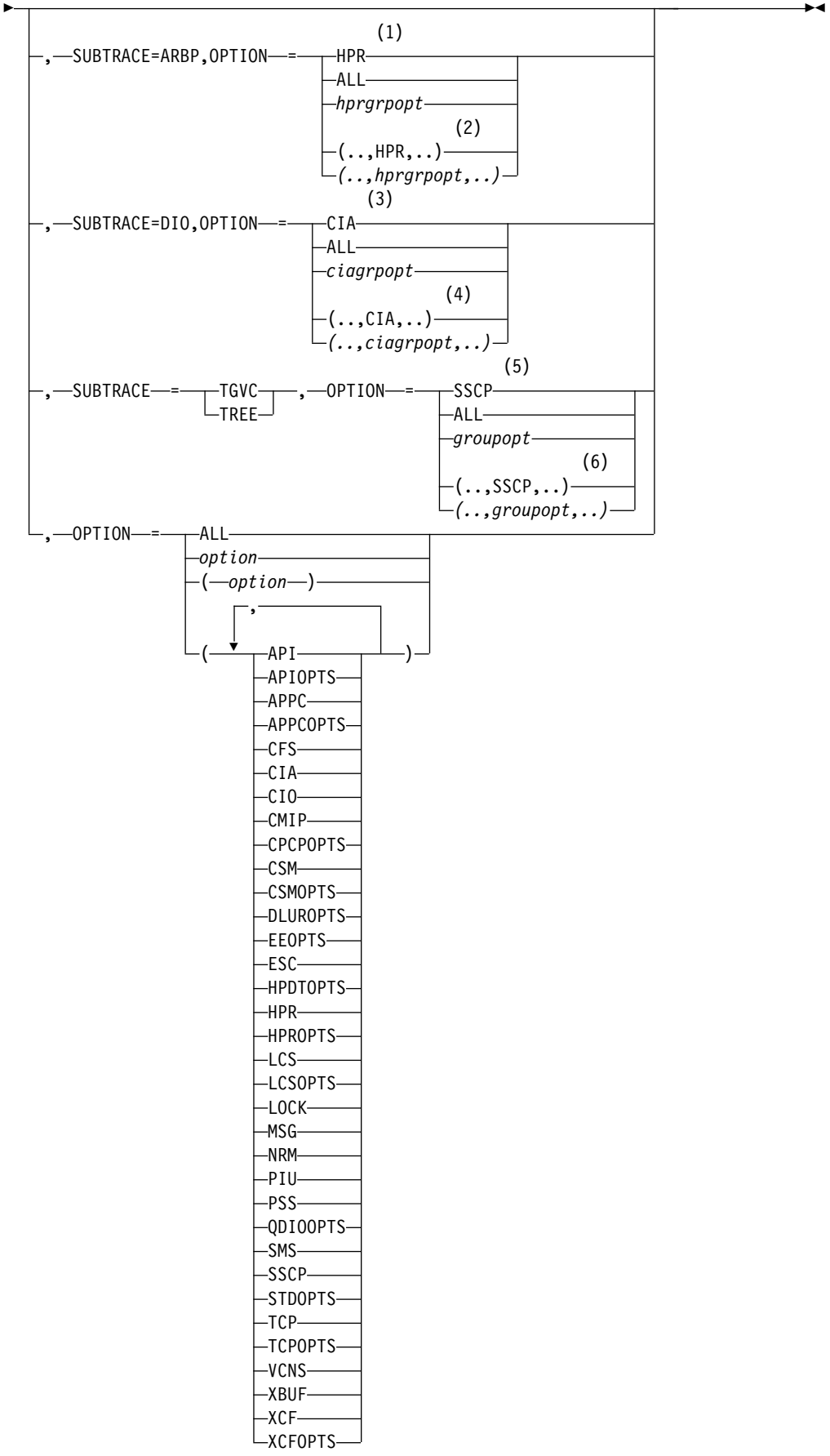


Start or modify a transmission group trace:

Start or modify a TSO user ID trace:

Start or modify the VTAM internal trace:




,SUBTRACE=ARBP,OPTION=
(1)
HPR
ALL
hprgrpopt
(2)
(..,HPR,..)
(..,hprgrpopt,..)
,SUBTRACE=DIO,OPTION=
(3)
CIA
ALL
ciagrpopt
(4)
(..,CIA,..)
(..,ciagrpopt,..)
,SUBTRACE=
TGVC
TREE
,OPTION=
(5)
SSCP
ALL
groupopt
(6)
(..,SSCP,..)
(..,groupopt,..)
,OPTION=
ALL
option
(option)
(
,
API
APIOPTS
APPC
APPCOPTS
CFS
CIA
CIO
CMIP
CPCPOPTS
CSM
CSMOPTS
DLUROPTS
EEOPTS
ESC
HPDTOPTS
HPR
HPROPTS
LCS
LCSOPTS
LOCK
MSG
NRM
PIU
PSS
QDIOOPTS
SMS
SSCP
STDOPTS
TCP
TCPOPTS
VCNS
XBUF
XCF
XCFOPTS
)

Notes:

1 When you specify SUBTRACE=ARBP and you code a single OPTION value, the OPTION value must be HPR, ALL, or one of the group options (*hprgrpopt*) that include HPR as an individual option equivalent. The applicable group options are DLUROPTS, EEOPTS, HPDTOPTS, HPROPTS, QDIOOPTS, and XCFOPTS.

2 When SUBTRACE=ARBP is coded and you code multiple trace options in parentheses, you must code either HPR or one of the group options (*hprgrpopt*) that include HPR as an individual option equivalent inside the parentheses.

3 When you specify SUBTRACE=DIO and you code a single OPTION value, the OPTION value must be CIA, ALL, or one of the group options (*ciagrpopt*) that include CIA as an individual option equivalent. The applicable group options are EEOPTS, HPDTOPTS, HPROPTS, QDIOOPTS, TCPOPTS and XCFOPTS.

4 When SUBTRACE=DIO is coded and you code multiple trace options in parentheses, you must code either CIA or one of the group options (*ciagrpopt*) that include CIA as an individual option equivalent inside the parentheses.

5 When you code SUBTRACE=TGVC or SUBTRACE=TREE and you code a single OPTION value, the OPTION value must be either SSCP, ALL, or one of the group options (*groupopt*), all of which include SSCP as an individual option equivalent. The group options are APIOPTS, APPCOPTS, CPCPOPTS, CSMOPTS, DLUROPTS, EEOPTS, HPDTOPTS, HPROPTS, LCSOPTS, QDIOOPTS, STDOPTS, TCPOPTS, and XCFOPTS.

6 When you code SUBTRACE=TGVC or SUBTRACE=TREE and you code multiple trace options in parentheses, you must code either SSCP or one of the group options (*groupopt*) inside the parentheses.

Abbreviations

Operand	Abbreviation
MODIFY	F
ALSNAME	ALS
AMOUNT=FULL	AMT=F
AMOUNT=PARTIAL	AMT=P
OPTION	OPT
OPTION=COMMAND	OPT=CMD
OPTION=CONNECTION	OPT=CON
OPTION=DEFINITION	OPT=DEF
OPTION=INTERFACES	OPT=INT
OPTION=MANAGEMENT	OPT=MGMT
OPTION=SESSION	OPT=SES
SAVE=YES	SAVE
SCOPE=ALL	EVERY or E
SCOPE=ONLY	NONE
TRACES	TRACE

When using an abbreviation in place of an operand, code the abbreviation exactly as shown in the table. For example, when coding the abbreviation for SCOPE=ALL, code only EVERY or E. Do not code SCOPE=E.

Purpose

The MODIFY TRACE command starts traces or modifies the parameters for currently running traces. VTAM traces are also started with the TRACE start option, as described in the z/OS Communications Server: SNA Resource Definition Reference.

Activation and use of VTAM traces have dependencies on the options used to start the system trace facility in each operating system environment. See the z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for a complete description of the system trace facility requirements, when to use these traces, and how to interpret the results.

General PIU trace (GPT) records are printed by the trace analysis program (ACFTAP) utility. For more information about ACFTAP, see z/OS Communications Server: ACF/TAP Trace Analysis Handbook.

Operands

procname

The procedure name for the command. If *procname* in the START command was specified as *startname.ident*, where *startname* is the VTAM start procedure and *ident* is the optional identifier, either *startname.ident* or *ident* can be specified for *procname*.

If *procname* in the START command was *startname*, *startname* must be specified for *procname*.

ALSNAME=adjacent_link_station_name

Applies only when TYPE=GPT and specifies the name of the adjacent link station through which you want tracing to occur. The adjacent link station name must be a PU in an NCP major node or a switched PU connected by an NCP link.

The LU can be traced over multiple connections; however, to do so, you must enter a separate command for each connection.

You do not need to specify the ALSNAME operand if either of the following situations is true:

- The ALS list has only one entry (and it is not ISTAPNPU). That entry is selected.
- The ALS list has two entries, one of which is ISTAPNPU. The entry other than ISTAPNPU is selected.

The command fails if ISTAPNPU is specified, or if ISTAPNPU is used by default because it is the only entry in the ALS list.

If no ALS list exists for the resource, specify the adjacent link station on the ALSNAME operand.

Use the DISPLAY ID=*lu_name*,SCOPE=ALL command to display all sessions for an independent LU and which adjacent link station list is used for each session.

AMOUNT

Applies only when TYPE=BUF. It determines whether VTAM starts a partial buffer contents trace or a full buffer contents trace for the specified node name.

You can run a partial buffer contents trace and a full buffer contents trace at the same time for different resources. (Issue a separate MODIFY TRACE command for each resource.) For example, you can start a partial buffer contents trace for an application program, with partial buffer contents tracing for some resources in session with the application program and full buffer contents tracing for other resources in session with the application program. When the level of tracing differs between two resources on opposite ends of a session (one is partial and the other is full), full buffer tracing is used.

You can switch between partial and full buffer tracing for the same resource by issuing additional MODIFY TRACE commands, without having to deactivate the trace.

AMOUNT=PARTIAL

Tells VTAM to record the data in trace records with a maximum size of 256 bytes. Each trace record contains a trace record header and data. Data that does not fit in a 256-byte trace record is lost.

AMOUNT=FULL

Tells VTAM to record all of the data transmitted in message buffers. Multiple trace records might be needed to record all of the data.

BFRNUM=*number*

- When you specify TYPE=VTAM,MODE=EXT this operand specifies the number of 8-K external trace buffers the VTAM internal trace is to allocate and use for generalized trace facility (GTF) processing. Values in the range of 2 - 50, or 0 can be specified. If you omit this option, the default value is 2. To ensure that enough buffers are available, specify a value that is twice as much as the number of processors in the central processing unit (CPU).

  When you specify a value in the range of 2 - 50, VTAM accumulates approximately 8 K of external trace data before sending the data to GTF.

  If 0 is specified or there is no buffer available for the trace record, VTAM sends each trace record to GTF as it is recorded. This can incur a significant system overhead, but might be necessary if you need individually timestamped records.

  If external trace recording is already active, and the new value specified for BFRNUM is less than the existing value, the number of buffers is not changed; if the new value is greater than the existing value, the number of the buffers is increased.
- When you specify TYPE=ROUTE, the BFRNUM operand specifies the maximum number of 40-K buffers to be allocated for the APPN route selection trace table. Values in the range of 1 - 500 can be specified. Storage for the route selection trace is not completely allocated when the trace is activated, but is allocated in 40-K buffers as it is needed. The APPN route selection trace is allocated in extended private storage.

  If you omit the BFRNUM option initially, the default for the maximum number of buffers is 100. After the APPN route selection trace is started, the BFRNUM operand does not have a default value. If successive MODIFY TRACE,TYPE=ROUTE commands are issued, the BFRNUM specification remains the same until you respecify it on a MODIFY command.

  If the BFRNUM value is too small, trace information might be lost as a result of wraparound in the route selection trace table. Also, if the BFRNUM value specified on the MODIFY TRACE,TYPE=ROUTE command is smaller than

the previous BFRNUM value, information is lost because the existing trace table is freed. If a MODIFY TRACE,TYPE=ROUTE command is entered with a BFRNUM value larger than the previous BFRNUM value, however, the storage allocated for the trace table will not be freed and additional buffers will be allocated as needed up to the new limit. If an attempt to allocate an additional block of trace table storage fails because of insufficient storage, the route selection trace table size might not reach the maximum size that you requested.

COUNT
Applies only when TYPE=LINE or TYPE=SIT. It specifies the number of bytes that are traced by either the NCP for a line trace (without the TG operand), or the communication scanner processor for the scanner interface trace. The COUNT operand has no effect on NTRI lines before NCP V5R2.1. NTRI always traces the same amount of data.

COUNT=number_of_bytes
Specifies the number of bytes of data to be traced. The value must be a decimal integer 0 - 254. COUNT=0 specifies that only the NCP control characters and none of the data is to be traced.

COUNT=ALL
Specifies that all of the data is to be traced.

DEVICE
Applies only when the ID operand is a TRLE that has the DATAPATH operand coded. Use DEVICE to start input/output trace on OSA-Express devices specified on the DATAPATH operand.

DEVICE=ALL
Specifies to turn on input/output trace on all devices in the DATAPATH list.

DEVICE=*hex_device_address*
Specifies to turn on input/output trace for a specific DATAPATH device.

FRAMES
Applies only when TYPE=NETCTLR. For a start/stop line, ALL is the only option. If DATA is specified on a start/stop line, it is ignored and the command proceeds as if ALL were specified. For SDLC and BSC lines, either DATA or ALL can be specified, with DATA being the default.

FRAMES=ALL
Specifies that all frames (meaning control and data frames) are to be traced by the cluster control unit.

FRAMES=DATA
Specifies that only data frames are to be traced by the cluster control unit.

ID=name
Specifies the name of the resource for which tracing is to be done. Only active resources can be traced. This operand does not apply when TYPE=MODULE or TYPE=VTAM.

Names of various types of resources can be specified, depending on the value of the TYPE operand. The different resources and the traces that can be specified for them (with the TYPE operand) are shown in Figure 18 on page 551 and are described in the following information.

For TYPE=BUF, TYPE=IO, TYPE=GPT, or TYPE=STATE, the name can be a network-qualified name. If *name* is an ACB name, and the ACB name matches the name on the APPL definition statement, then you can use a network-qualified ACB name.

For TYPE=BUF, TYPE=IO, or TYPE=STATE for a CDRM, you can specify a network-qualified name, but this does not remove the restriction that the non-network-qualified CDRM name must be unique across networks.

For TYPE=BUF, TYPE=IO, or TYPE=STATE, the name can be a model resource (APPL or CDRSC). If SCOPE=ALL is specified, the command also applies to the clone resources created from the model. If SCOPE=ONLY is specified, current clone resources are unaffected, but future clone resources will be affected when they are created.

For TYPE=QDIOSYNC, the ID operand specifies the TRLE name of the OSA-Express2 adapter for which diagnostic data synchronization and filtering is to be started. Specify ID=* to start QDIOSYNC for all TRLEs that define OSA-Express2 adapters. When ID=* is specified with SAVE=NO, ID=* indicates that the QDIOSYNC command is to be applied to all currently active TRLEs that define OSA-Express2 adapters. When ID=* is specified with SAVE=YES, ID=* indicates that the QDIOSYNC command is to be applied to all currently active TRLEs that define OSA-Express2 adapters and to those that are activated by this VTAM in the future.

When multiple QDIOSYNC NOTRACE or TRACE commands are specified, the last one that is applicable to a specific *trle_name* value takes precedence. For example, TRACE TYPE=QDIOSYNC,ID=TRLE1 requests synchronization for a single OSA-Express2 adapter, but the request is canceled if it is followed by NOTRACE TYPE=QDIOSYNC, ID=*. TRACE TYPE=QDIOSYNC, ID=* requests synchronization of all OSA-Express2 adapters and, if it is followed by NOTRACE TYPE=QDIOSYNC,ID=TRLE1, results in synchronization of all OSA-Express2 adapters except TRLE1.

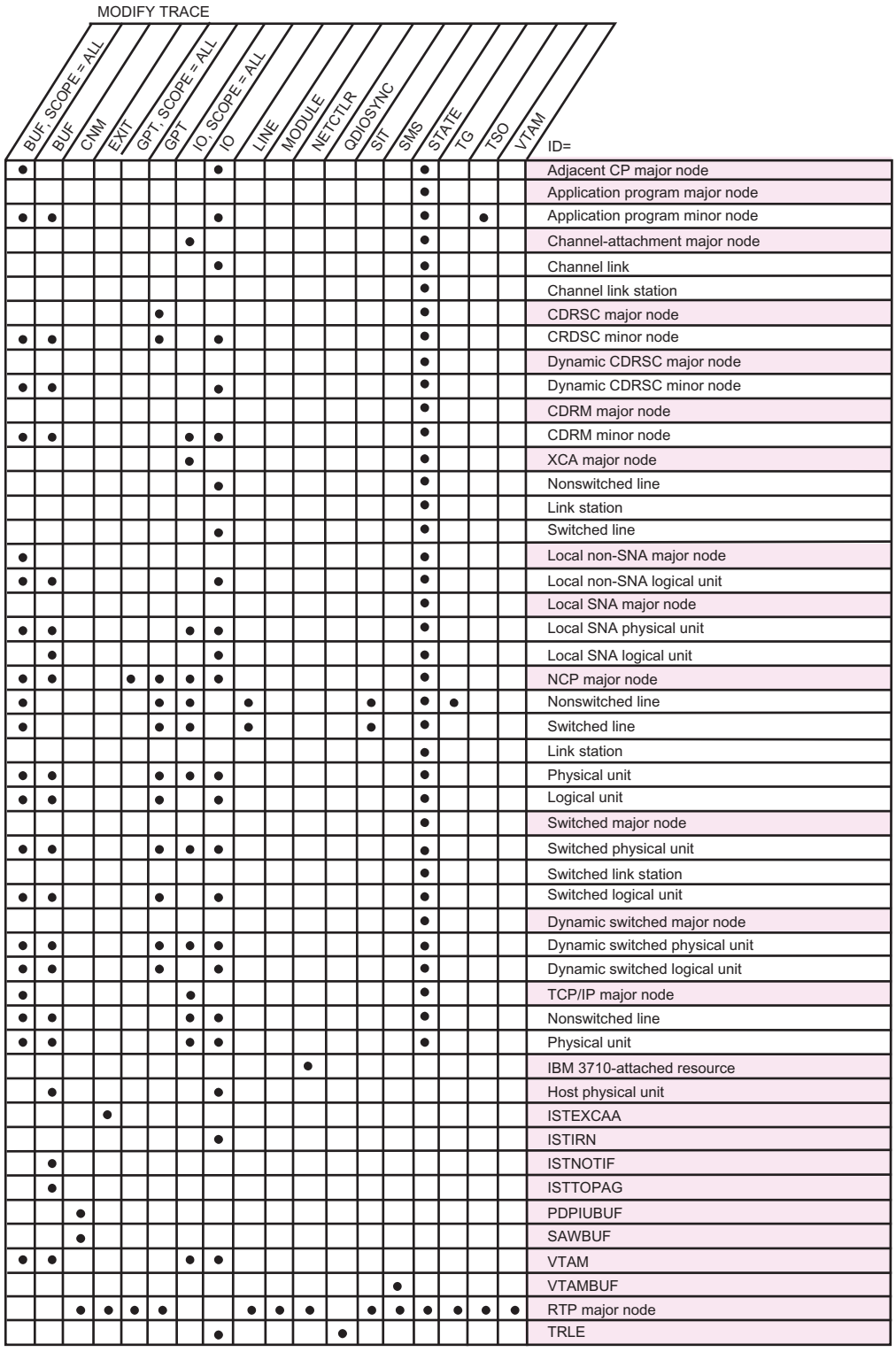


Figure 18. Resource and trace reference

- For **TYPE=BUF or TYPE=IO**, any of the following names can be specified along with the SCOPE=ALL operand to trace message activity with the named resource and, if applicable, all of the resource's subordinate nodes:

- The name of an NCP major node
- The name of the following major nodes (only TYPE=IO,SCOPE=ALL can be specified):
  - Channel-attachment major node
  - XCA major node
- The name of a line attached to a communication adapter (only TYPE=IO,SCOPE=ONLY can be specified)
- The name of a switched line that has a physical unit attached to it
- The name of a TRLE (only TYPE=IO,SCOPE=ONLY can be specified)

  Restriction: I/O tracing is not supported for a TRLE that represents a 10GbE RoCE Express feature or an internal shared memory (ISM) device.
- The name of one of following types of physical units:
  - Channel-attached SNA physical unit
  - Switched physical unit
- The name of a logical unit
- The name of the host CDRM

  Note: If you do a trace for a host CDRM, any subordinate minor nodes also have trace turned on.

Any of the following names can be specified to trace message activity with the named resource:

- Host physical unit (for a trace of all PIUs between this host and another PU type 4 or PU type 5)
- ISTIRN (with TYPE=IO only, for an IO trace of all PIUs passing through this host that are received from a channel-attached PU type 4 or type 5 and are being sent to another channel-attached PU type 4 or type 5)
- VTAM (for a trace of all SSCP sessions)
- The name of an NCP
- The name of a logical unit (including application programs)
- The name of a local non-SNA minor node
- The name of a CDRM (only in a multiple-domain or multiple-network environment)
- The name of a CDRSC
- The name of the internal or external CMIP application program (for TYPE=BUF only). For the VTAM topology agent, *node_name* is ISTTOPAG. For notification services, *node_name* is ISTNOTIF. For external CMIP application programs, *node_name* is the application name defined as the ACB name of the application program major node. In the following example, APPL1 is the name of the CMIP application program, as defined in the name field of the APPL definition statement.

  ```
  APPL1     APPL   PRTCT=ADRAPL01
  ```

The host CP can be traced as an application program minor node, and adjacent CPs can be traced as CDRSC minor nodes.

- For **TYPE=CNM**, the ID operand specifies one of the following values:
  - PDPIUBUF, to start the problem determination PIU buffer trace
  - SAWBUF, to start the session awareness buffer trace
- For **TYPE=EXIT**, the ID operand is required and must be specified as ISTEXCAA, ISTEXCCS, or ISTEXCDM.

- For **TYPE=GPT**, the ID operand specifies the name of the NCP resource for which tracing is to be done:
  - An NCP major node (and all of its resources) that is active or pending active
  - An NCP switched or nonswitched line

    Note: The ID operand of MODIFY TRACE cannot specify an NCP switched line that is a switched subarea connection.
  - An active LU that has been dynamically reconfigured within the NCP
  - An active PU on an NCP switched line
  - An active or inactive PU on an NCP nonswitched line
  - An active PU that is dynamically reconfigured within the NCP
  - An active or inactive LU associated with an active PU on a switched line
  - An active or inactive LU associated with a PU (active or inactive) on a nonswitched line
  - An active or inactive independent LU associated with a PU (ALS) in an NCP major node or a switched PU connected by an NCP link. The state (active or inactive) of the PU with which the independent LU is associated must be as follows:
    - If it has been dynamically reconfigured within the NCP, the PU must be active
    - If it is on an NCP switched line, the PU must be active.
    - If it is on an NCP nonswitched line, the PU can be either active or inactive.

  The SSCP and host CP are not valid resources for a GPT trace, but the adjacent CP can be traced as a CDRSC minor node.
- For **TYPE=NETCTLR**, the ID operand specifies the name of the physical unit representing the device for which the trace is to be started. (VTAM is not required to own or have knowledge of the 3710.) VTAM sends the name of the PU specified on the ID operand to the 3710 specified on the PU operand.

  If a 3710 is to be simultaneously traced over more than one line, use a separate MODIFY TRACE command to start each trace.

  Note: It is not necessary that the resource specified by the ID operand be another 3710.
- For **TYPE=LINE or TYPE=SIT**, the ID operand specifies the name of the line for which tracing is to be done.

  ID cannot specify a line attached to a communication adapter or the name of a transmission group through a communication adapter.
- For **TYPE=SMS** the ID operand is optional. If it is omitted, ID=VTAMBUF will be used for an SMS trace.
- For **TYPE=STATE**, the ID operand specifies the name of the resource for which state tracing is to be done.
- For **TYPE=TG**, the ID operand specifies the name of a nonswitched line currently within the transmission group to be traced. All the lines in the transmission group are traced as if they were a single logical line.
- For **TYPE=TSO**, the ID operand specifies the TSO user ID for which tracing is to be done.

IDTYPE
Specifies the type of resource that the ID operand names. If several types of resources share the same name, IDTYPE identifies which resources the command should act on. IDTYPE applies to TYPE=BUF, TYPE=IO, TYPE=GPT, and TYPE=STATE.

IDTYPE=CP
Starts tracing for the control point (CP) with the name specified on the ID operand. The CP that is traced can be the host CP or a CDRSC representing an adjacent CP.

IDTYPE=SSCP
Starts tracing for the system services control point (SSCP) with the name specified on the ID operand.

IDTYPE=RESOURCE
Starts tracing for a CP, an SSCP, or another resource with the name specified on the ID operand. If both an SSCP and a CP are found, VTAM starts tracing for both of them.

LENGTH
Applies only when the DEVICE operand is specified and the ID operand is a TRLE that has the DATAPATH operand coded. Use LENGTH to specify the number of bytes from each packet to trace. Valid values are 56 - 9016. Values are rounded up to 56 and values above 9016 are rounded down to 9016. All values are rounded up, if necessary, to an even multiple of 28.

Note: The default value is 272 for a TRLE that has the DATAPATH operand coded.

LINE=line_name
Applies only to TYPE=NETCTLR. It specifies the name of a link that is attached to the 3710 that is to be traced. The 3710 performing the trace (named on the PU operand) copies the SDLC, BSC, and S/S data link control frames that are transmitted or received on that link for the physical unit named by the ID operand. VTAM has no knowledge of this link. VTAM sends the name of the link specified on the LINE operand to the 3710 specified on the PU operand.

MODE
Applies only to TYPE=VTAM. It specifies that the VTAM internal trace is to record its data on an internal, wraparound table (MODE=INT) or an external trace file (MODE=EXT).

You can record trace data internally and externally at the same time. If required, you can have different sets of trace options active for internal and external recording. VTAM always runs with MODE=INT and the default trace options, regardless of whether you request tracing.

You must run specific operating system utilities to trap, format, and view external trace output. See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information about use of these operating system utilities.

Do not specify MODE=EXT and SIZE on the same command.

MODE=INT
Specifies that the VTAM internal trace is to record its data on an internal, wraparound table.

MODE=EXT
Specifies that the VTAM internal trace is to record its data on an external trace file and on an internal, wraparound table.

OPTION
Applies to TYPE=EXIT, TYPE=MODULE, TYPE=QDIOSYNC, TYPE=STATE and TYPE=VTAM.

For **TYPE=EXIT**, OPTION specifies the functions of the session management exit (SME), directory services management exit (DSME), or configuration services XID exit for which tracing is to be started.

If more than one option is selected, separate them with commas and enclose the list in parentheses; for example OPTION=(BEGIN,INITAUTH,ACCTING).

For **TYPE=MODULE**, OPTION specifies the types of processing modules for which tracing is to be started.

If more than one option is selected, separate them with commas and enclose the list in parentheses; for example OPTION=(COMMAND,SESSION).

For **TYPE=QDIOSYNC**, OPTION specifies the scope and filter to be applied by the OSA-Express2 adapter. OPTION specifies the devices and the direction for which diagnostic data is to be gathered.

For **TYPE=STATE**, OPTION specifies the types of resources for which resource states are to be recorded. The data is recorded using the mode (internal or external) specified for the SSCP VIT option.

If more than one option is selected, separate them with commas and enclose the list in parentheses; for example OPTION=(APPL,GROUP,NCP).

For **TYPE=VTAM**, OPTION specifies the VTAM internal functions for which trace data is to be recorded.

The API, CIO, MSG, NRM, PIU, and SSCP VIT options are kept active by VTAM for internal recording (MODE=INT). If you stop them, VTAM immediately restarts them. For external recording (MODE=EXT), there are no default options. You can start or stop any options.

Note: Although the default options are always active, these options do not appear in DISPLAY TRACES output unless you have specified them on the MODIFY TRACE command or the TRACE,TYPE=VTAM start option.

If more than one option is selected, separate them with commas and enclose the list in parentheses; for example OPTION=(API,NRM,SSCP). For information about what is traced for each internal function, see the z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT.

OPTION=ALL
Applies to TYPE=EXIT, TYPE=MODULE, TYPE=STATE, and TYPE=VTAM.

Note: Turning on all traces slows performance.

For TYPE=EXIT, it starts the tracing of all functions.

For TYPE=MODULE, it starts the tracing of all the modules shown on the OPTION operand for which TYPE=MODULE apply.

For TYPE=STATE, it starts the tracing of resource states for all of the resource types shown on the OPTION operand for which TYPE=STATE apply.

For TYPE=VTAM, it starts the VTAM internal trace for all of the VTAM internal functions for which the VTAM internal trace is available. Exception trace entries continue to be recorded.

For **TYPE=EXIT** where ID=ISTEXCAA, you can also specify the following options:

OPTION=ALL
Starts the tracing of all functions.

OPTION=ACCTING
Starts tracing the initial and final accounting function of the session management exit (SME).

OPTION=ADJSSCP
Starts tracing the adjacent SSCP selection function of the session management exit (SME).

OPTION=ALIAS
Starts tracing the alias translation function of the session management exit (SME).

OPTION=ALS
Starts tracing the adjacent link station function of the session management exit (SME).

OPTION=BEGIN
Starts tracing the begin function of the session management exit (SME).

OPTION=END
Starts tracing the end function of the session management exit (SME).

OPTION=GWPATH
Starts tracing the gateway path list function of the session management exit (SME).

OPTION=INITAUTH
Starts tracing the initial authorization function of the session management exit (SME).

OPTION=REPL
Starts tracing the exit replacement function of the session management exit (SME).

OPTION=SECAUTH
Starts tracing the secondary authorization function of the session management exit (SME).

OPTION=VRSEL
Starts tracing the virtual route selection function of the session management exit (SME).

OPTION=XRF
Starts tracing the XRF session switch function of the session management exit (SME).

For **TYPE=EXIT** where ID=ISTEXCCS, you can also specify the following options:

OPTION=ALL
Starts the tracing of all functions.

OPTION=BEGIN
Starts tracing the begin function.

OPTION=CONNSTAT
Starts tracing the connection status.

OPTION=DYNA_XID
Starts tracing the XIDs for dynamic PUs function.

OPTION=END
Starts tracing the end function.

OPTION=PRED_XID
Starts tracing the XIDs for predefined PUs function.

For **TYPE=EXIT** where ID=ISTEXCDM, you can also specify the following options:

OPTION=ALL
Starts the tracing of all the functions.

OPTION=ADS_SEL
Starts tracing the alternate central directory server selection function.

OPTION=BEGIN
Starts tracing the begin function.

OPTION=BN_SEL
Starts tracing the border node selection function.

OPTION=CDS_SEL
Starts tracing the central directory server selection function.

OPTION=CRR_SEL
Starts tracing the central resource registration selection function.

OPTION=END
Starts tracing the end function.

OPTION=ICN_SEL
Starts tracing the interchange node selection function.

OPTION=INITAUTH
Starts tracing the initial authorization function.

OPTION=REPL
Starts tracing the exit replacement function

For **TYPE=MODULE**, you can also specify the following options:

OPTION=COMMAND
Starts tracing modules involved in command processing.

OPTION=CONNECTION
Starts tracing modules involved in setting up connections between nodes.

OPTION=DEFINITION
Starts tracing modules involved in resource definition processing.

OPTION=INTERFACES
Starts tracing modules involved in the interface with the host SSCP or the host CP.

OPTION=MANAGEMENT
Starts tracing modules involved in network management.

OPTION=NOEXIT
Specifies that module exits are not traced for modules associated with other OPTION values for TYPE=MODULE. Module exits are not traced for

any modules until a subsequent MODIFY NOTRACE,TYPE=MODULE,OPTION=NOEXIT command is issued.

Starting a module trace for any OPTION with TYPE=MODULE starts the tracing of the module exits also, unless you specify OPTION=NOEXIT.

OPTION=PURGE
Causes all information currently held in module tracing buffers to be written to VTAM internal trace (VIT) entries. Upon completion of the command, new information is written to the module tracing buffers.

OPTION=SESSION
Starts tracing modules involved in session establishment.

For **TYPE=QDIOSYNC**, you can specify the following options:

OPTION=ALLIN
Indicates that the adapter should gather diagnostic data for all devices, including any that might be controlled by other operating systems. This option also indicates that the adapter should collect records pertinent to events and data flowing from the adapter to the host. Code the value OPTION=ALLIN only when advised by IBM service to do so.

OPTION=ALLINOUT
Indicates that the adapter should gather diagnostic data for all devices, including any that might be controlled by other operating systems. This option also indicates that the adapter should collect both inbound and outbound diagnostic data.

OPTION=ALLOUT
Indicates that the adapter should gather diagnostic data for all devices, including any that might be controlled by other operating systems. This option also indicates that the adapter should collect records pertinent to events and data flowing from the host to the adapter. Code OPTION=ALLOUT only when advised by IBM service to do so.

OPTION=IN
Indicates that the adapter should gather diagnostic data for devices defined to this VTAM only. This option also indicates that the adapter should collect records pertinent to events and data flowing from the adapter to the host. Code OPTION=IN only when advised by IBM service to do so.

OPTION=INOUT
Indicates that the adapter should gather diagnostic data for devices defined to this VTAM only. This option also indicates that the adapter should collect both inbound and outbound diagnostic data. Code OPTION=INOUT only when advised by IBM service to do so.

OPTION=OUT
Indicates that the adapter should gather diagnostic data for devices defined to this VTAM only. This option also indicates that the adapter should collect records pertinent to events and data flowing from the host to the adapter. Code OPTION=OUT only when advised by IBM service to do so.

For **TYPE=STATE**, you can also specify the following options:

OPTION=ADJCP
Starts tracing the states of all adjacent control points.

OPTION=APPL
Starts tracing the states of all application programs.

OPTION=CDRM
Starts tracing the states of all CDRMs.

OPTION=CDRSC
Starts tracing the states of all CDRSCs.

OPTION=GROUP
Starts tracing the states of all line groups.

OPTION=LINE
Starts tracing the states of all lines.

OPTION=LNKST
Starts tracing of link stations.

OPTION=LU
Starts tracing the states of all logical units.

OPTION=NCP
Starts tracing the states of all NCPs.

OPTION=PU
Starts tracing the states of all physical units.

For **TYPE=VTAM**, you can also specify the following options:

OPTION=API
Starts tracing the application programming interface.

OPTION=APIOPTS
Starts tracing events related to the application programming interface (API). Specifying this value is equivalent to specifying OPTION=(API,MSG,NRM,PIU,PSS,SMS,SSCP).

OPTION=APPC
Starts tracing LU 6.2 communication.

OPTION=APPCOPTS
Starts tracing events related to LU 6.2 application programs. Specifying this value is equivalent to specifying OPTION=(API,APPC,MSG,NRM,PIU,PSS,SMS,SSCP).

OPTION=CFS
Starts tracing coupling facility services.

OPTION=CIA
This option helps isolate problems related to channel I/O. CIA entries are the remaining trace records from the CIO option.

OPTION=CIO
Starts tracing channel I/O for channel-attached devices and for lines attached to a communication adapter.

OPTION=CMIP
Starts tracing internal events in CMIP services and the VTAM topology agent.

OPTION=CPCPOPTS
Starts tracing events related to CP-CP sessions. Specifying this value is equivalent to specifying OPTION=(API,APPC,MSG,NRM,PIU,PSS,SMS,SSCP).

OPTION=CSM
Starts tracing of the communications storage manager.

OPTION=CSMOPTS
Starts tracing events related to communications storage manager (CSM). Specifying this value is equivalent to specifying OPTION=(API,APPC,CIO,CSM,MSG,NRM,PIU,PSS,SMS,SSCP,XBUF).

OPTION=DLUROPTS
Starts tracing events related to dependent LU requester (DLUR). Specifying this value is equivalent to specifying OPTION=(API,APPC,HPR,MSG,NRM,PIU,PSS,SMS,SSCP).

OPTION=EEOPTS
Starts tracing events related to Enterprise Extender (EE). Specifying this value is equivalent to specifying OPTION=(CIA,CIO,HPR,MSG,NRM,PIU,PSS,SMS,SSCP,TCP).

OPTION=ESC
Starts tracing execution sequence control.

OPTION=HPDTOPTS
Starts tracing events related to high performance data transfer (HPDT). Specifying this value is equivalent to specifying OPTION=(CIA,CIO,HPR,MSG,PIU,PSS,SMS,SSCP).

OPTION=HPR
Starts tracing for HPR.

OPTION=HPROPTS
Starts tracing events related to high performance routing (HPR). Specifying this value is equivalent to specifying OPTION=(API,APPC,CIA,CIO,HPR,MSG,NRM,PIU,PSS,SMS,SSCP).

OPTION=LCS
Starts tracing LAN channel stations.

OPTION=LCSOPTS
Starts tracing events related to LAN channel station (LCS). Specifying this value is equivalent to specifying OPTION=(CIO,LCS,MSG,NRM,PIU,PSS,SMS,SSCP).

OPTION=LOCK
Starts tracing locking.

OPTION=MSG
Starts tracing messages.

OPTION=NRM
Starts tracing network resource management

OPTION=PIU
Starts tracing path information units.

OPTION=PSS
Starts tracing process scheduling services.

OPTION=QDIOOPTS
Starts tracing events related to queued direct I/O (QDIO). Specifying this value is equivalent to specifying OPTION=(CIA,CIO,HPR,MSG,NRM,PIU,PSS,SMS,SSCP).

OPTION=SMS
Starts tracing Storage Management services.

OPTION=SSCP
Starts tracing the system services control point.

OPTION=STDOPTS
Starts tracing events related to the application programming interface, channel I/O, messages, network resource management, path information units, process scheduling services, Storage Management services, and the system services control point. Specifying this value is equivalent to specifying OPTION=(API,CIO,MSG,NRM,PIU,PSS,SMS,SSCP).

OPTION=TCP
Starts tracing the Enterprise Extender events.

OPTION=TCPOPTS
Starts tracing events related to TCP/IP. Specifying this value is equivalent to specifying OPTION=(CIA,CIO,MSG,NRM,PIU,PSS,SMS,SSCP,TCP).

OPTION=VCNS
Starts tracing VTAM common network services.

OPTION=XBUF
Starts tracing of extended buffer list information.

OPTION=XCF
Starts tracing XCF communication.

OPTION=XCFOPTS
Starts tracing events related to the cross-system coupling facility (XCF). Specifying this value is equivalent to specifying OPTION=(CIA,CIO,HPR,MSG,NRM,PIU,PSS,SMS,SSCP,XCF).

PU=3710_pu_name
Applies only when TYPE=NETCTLR. It specifies the name of the IBM 3710 Network Controller that is to perform the trace. VTAM rejects the command if the physical unit is not known to VTAM.

SAVE
Applies to TYPE=BUF, TYPE=IO, TYPE=QDIOSYNC, and TYPE=STATE. It specifies whether the trace command should be saved for the resource named on the ID operand.

SAVE=YES
VTAM saves the trace command for the resource named on the ID operand. If the resource exists when this command is issued, the trace starts immediately. If the resource does not exist when this command is issued, VTAM saves the trace command and starts the trace when the resource is defined.

Note: For TYPE=BUF, TYPE=IO, and TYPE=STATE, if you start a trace with IDTYPE=RESOURCE and a CP or an SSCP (but not both) exists when the command is issued, VTAM starts the trace for the existing resource and saves the trace commands for both resources. If both a CP and an SSCP exist when the command is issued, VTAM starts tracing for them immediately.

You can also issue this command to update a previously saved trace command.

For TYPE=QDIOSYNC:

- If ID=*trlename* is specified, any saved command from a previous TRACE TYPE=QDIOSYNC command or start option for the TRLE specified by the *trle_name* value is deleted.

- If ID=* is specified, all saved commands from previous TRACE TYPE=QDIOSYNC commands and start options are deleted.

Use the MODIFY NOTRACE command to delete a saved trace command. VTAM will not delete a saved trace command until you issue a MODIFY NOTRACE command for it, even though the resource might be created and freed or activated and deactivated several times. Saved trace commands are lost when VTAM is halted and restarted.

SAVE=NO
Does not save the MODIFY TRACE command. If the resource does not exist when you issue MODIFY TRACE, the command fails.

SCOPE
Applies when TYPE=BUF, TYPE=IO, or TYPE=GPT. It specifies the scope of the trace.

You can specify the SCOPE operand for TYPE=GPT, but it is meaningful only for the NCP node. SCOPE=ALL is assumed for a GPT trace of all other node types.

SCOPE=ALL
Starts traces for all nodes subordinate to the specified node. If an LU that is subordinate to a node is an independent LU, it is not considered to be subordinate to the node for the purpose of tracing.

SCOPE=ALL is not valid for the host PU trace or for the host intermediate routing node trace (ID=ISTIRN). If SCOPE=ALL is specified, VTAM issues a message and uses SCOPE=ONLY.

For an I/O trace of a channel-attached NCP, SCOPE=ALL provides a trace of all channel I/O, including network message traffic routed through the channel-attached NCP.

If the specified node is a model application, SCOPE=ALL turns on the trace option for the model application and starts traces for all existing dynamic applications created using the model. Traces will be started for future dynamic applications created using the model.

SCOPE=ONLY
Starts a trace only for the specified node.

SCOPE=ONLY on a GPT trace command for the NCP PU limits the trace to RUs that flow on the SSCP-PU session for the NCP.

If the specified node is a model application, SCOPE=ONLY turns on the trace option for the model application. Traces for all existing dynamic applications created using the model are unaffected. Traces will be started for future dynamic applications created using the model.

SIZE=*size*
Applies only when you specify TYPE=VTAM,MODE=INT. The size operand specifies the number of megabytes to be allocated for the internal trace table. Valid values are in the range 4M - 2048M. The VTAM internal trace table is allocated in 64-bit common (HVCOMMON) storage.

If the VTAM internal trace is not already started and you omit this option, the default size is 4M.

After the VTAM internal trace is started, the SIZE operand does not have a default value. If successive MODIFY commands change other options, the SIZE specification remains the same until you respecify it on a MODIFY command.

If the SIZE value is too small, trace information might be lost as a result of wraparound in the internal trace table. Also, if the SIZE operand specifies a size different from the current table size, information is lost because the trace table is freed when another table with a new size is obtained. When an attempt to increase the SIZE value fails because of insufficient storage, the internal trace table size is set to the minimum size, not the size that you requested.

Restriction: If you specify a SIZE value that is larger than the default value, z/OS will perform paging on portions of the VIT table. Before you specify a large SIZE value, ensure that you have sufficient real or auxiliary storage to contain the entire VIT. Failure to ensure that sufficient storage might result in an auxiliary storage shortage. If an SVC dump is taken that includes common storage, the size of the dump data set also increases. You must also take the increase in the size of the dump data set into consideration.

SUBTRACE
Specifies that SUBTRACE can be used to turn on a subset of trace entries under a trace option. Of the SUBTRACE types defined, subtrace DIO is defined under the CIA trace option, subtrace TREE, and TGVC are defined under the SSCP trace option, and subtrace ARBP is defined under the HPR trace option.

Note: All of the SUBTRACE options are defaulted to off. They can generate many records in the VTAM trace and can incur a significant overhead, but may be necessary in some cases for diagnostic purposes. It is not recommended to activate them at VTAM start time. If used, the SUBTRACE options should be turned off when the necessary trace output has been obtained.

SUBTRACE=ARBP
Specifies that OPTION is a required keyword when SUBTRACE is specified and HPR must be one of the trace options specified when SUBTRACE=ARBP is coded. After subtrace ARBP is activated, the following trace records will be generated for the ARB algorithm processing: ARBR (Generated when ARB Responsive Mode algorithm is used) and ARBB (Generated when ARB Base Mode algorithm is used).

SUBTRACE=DIO
Specifies that OPTION is a required keyword when SUBTRACE is specified and CIA must be one of the trace options specified when SUBTRACE=DIO is coded. After subtrace DIO is activated, the following trace records may be generated for QDIO and Hipersockets processing: QAPL, QDIP and QSRB.

SUBTRACE=TGVC
Specifies that OPTION is a required keyword when SUBTRACE is specified and SSCP must be one of the trace options specified when SUBTRACE=TGVC is coded. After subtrace TGVC is activated, the following trace records will be generated for various TG Vector requests: TGVC and TGV2. If large amounts of data are being traced, additional TGVC records (plus subsequent TGV2 records) may occur.

SUBTRACE=TREE
Specifies that OPTION is a required keyword when SUBTRACE is specified and SSCP must be one of the trace options specified when SUBTRACE=TREE is coded. After subtrace TREE is activated, the following trace records will be generated for routing trees used by APPN route computation: TRRT, TRR2, TRR3, TRR4, TRR5, HLST, and HLS2.

SYNCID
Valid for TYPE=QDIOSYNC. The OSA-Express2 uses this value as part of an identifier when it captures diagnostic data.

Restriction: If you specify a value for SYNCID, it must conform to the rules for names. See z/OS Communications Server: SNA Resource Definition Reference for more information.

TRACEPT=trace_point_id
Applies to TYPE=SIT and is valid only if you are tracing connectivity subsystem (CSS) resources on an IBM 3745 Communication Controller. This operand specifies the point in the microcode at which tracing should be activated. If you omit this operand, tracing is done for all valid trace points. Using the TRACEPT operand, you can limit the tracing to a single trace point if too much output is being produced.

VTAM accepts any integer in the range 1 - 255; however, only a few values are defined by the NCP. For information about which values are defined and what they mean, see the *NCP, SSP, and EP Diagnosis Guide*.

TYPE
Specifies the kind of trace that is to be affected. More than one kind of trace can be active at the same time, but you must start or change each trace with a separate MODIFY TRACE command.

TYPE=BUF
Starts the tracing of text that passes through VTAM buffers on the way to or from the node identified by the ID operand. The SCOPE operand can be used to extend the scope of the trace to all nodes subordinate to the specified node. This trace is useful when one of the logical units in the session is an application program in this domain.

TYPE=CNM
Starts a communication network management trace.

Note: When this option is specified, the generalized trace facility (GTF) must be active with the TRACE=USR option specified.

TYPE=EXIT
Starts the tracing of functions of the session management exit (SME).

TYPE=GPT
Starts an NCP generalized PIU trace (GPT) for the resources identified by the ID operand.

Note: The ID operand of MODIFY TRACE cannot specify:

- An NCP switched line that is a switched subarea connection
- A dynamic CDRSC

TYPE=IO
Starts a trace of I/O activity associated with the node identified by the ID operand. The SCOPE operand can be used to extend the scope of the trace to all nodes subordinate to the specified node. In addition, for an NCP major node with an active channel attachment, the SCOPE=ALL operand provides a trace of all I/O going across the channel, including cross-domain session I/O.

Note: The external VIT is now used to record the IO trace entries. PIU, NLPI, NLPO, LSNA, and MPTNFMT entries may be written for a specific IO trace invocation.

TYPE=LINE
Starts an NCP line trace for the line identified by the ID operand.

TYPE=MODULE
Starts module tracing for the options specified on the OPTION operand.

TYPE=NETCTLR
Sends a trace request to the 3710 named on the PU operand.

TYPE=QDIOSYNC
Use TYPE=QDIOSYNC to synchronize and optionally filter OSA-Express2 diagnostic data.

Arming the OSA-Express2 adapter directs it to capture diagnostic data when there is an unexpected loss of host connectivity. Diagnostic data is also captured when the following situations occur:

- The VTAM-supplied message processing facility (MPF) exit IUTLLCMP is driven.
- Either the VTAM or TCP/IP functional recovery routine (FRR) is driven with the ABEND06F abend. ABEND06F is the result of a SLIP PER trap command specifying ACTION=RECOVERY.

  Restriction: The SLIP must be a SLIP PER trap in order to specify ACTION=RECOVERY.
  See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Proceduresfor more information about the QDIOSYNC facility.

TYPE=ROUTE
Starts the APPN route selection trace.

TYPE=SIT
Starts a scanner interface trace (SIT) through the communication scanner processor located in the IBM 3720 or 3745 Communication Controller containing the NCP identified by the line specified by the ID operand.

The scanner interface trace and the NCP line trace can be started separately, and can be active at the same time.

TYPE=SMS
Starts a Storage Management services (SMS) trace to record VTAM buffer pool usage data.

TYPE=STATE
Starts a resource state trace to record the changing states of resources.

TYPE=TG
Starts an NCP transmission group trace for the transmission group (TG) containing the NCP line identified by the ID operand. A line is part of a transmission group only when both the line and its subordinate link station are active. A transmission group trace can be started by naming any line within the transmission group. When a transmission group trace is started, another trace of the same transmission group cannot be requested by naming the same or another line within the transmission group in another MODIFY TRACE command.

If the line or its link station subsequently fails or is deactivated (that is, if the line is removed from the transmission group), the transmission group

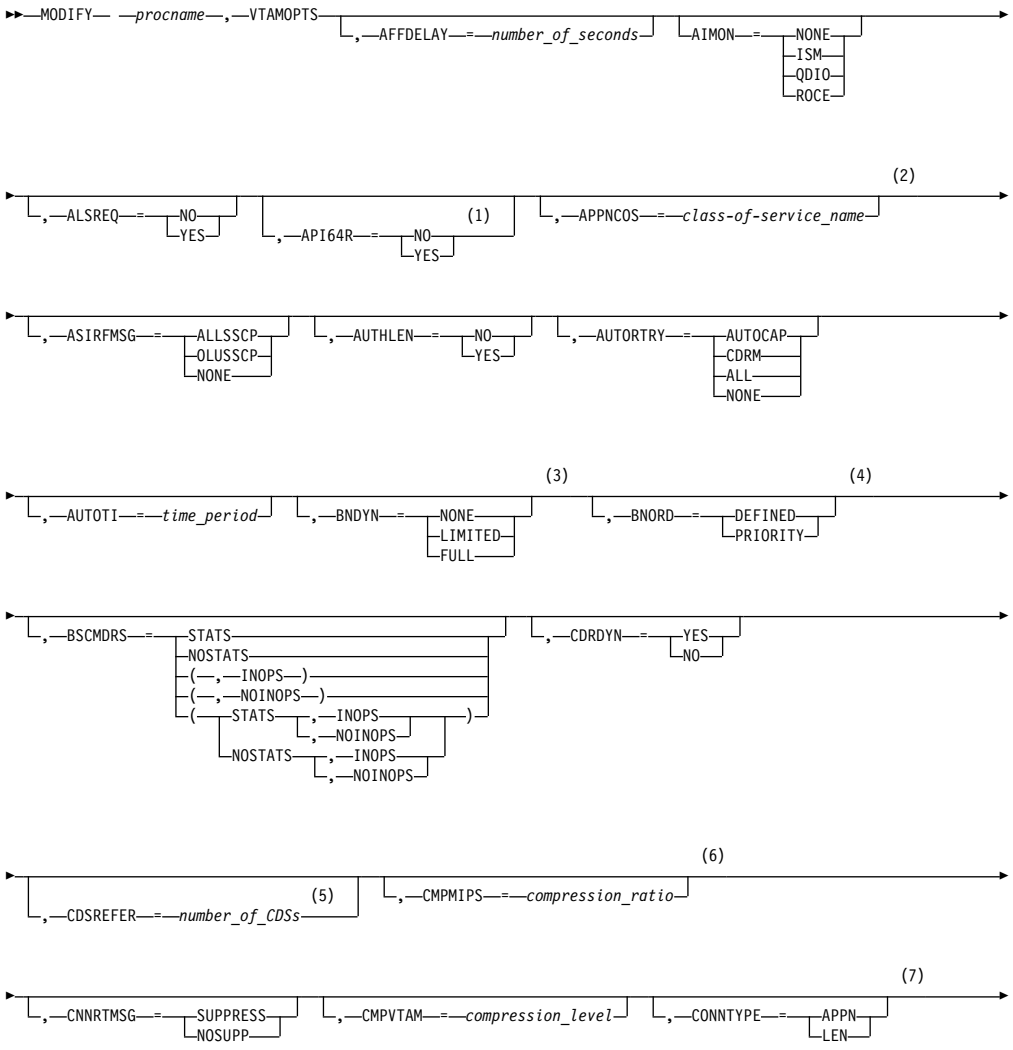
trace is ended, even though the transmission group continues to operate if there are any remaining lines in the transmission group. The trace can be restarted, naming another line in the transmission group.

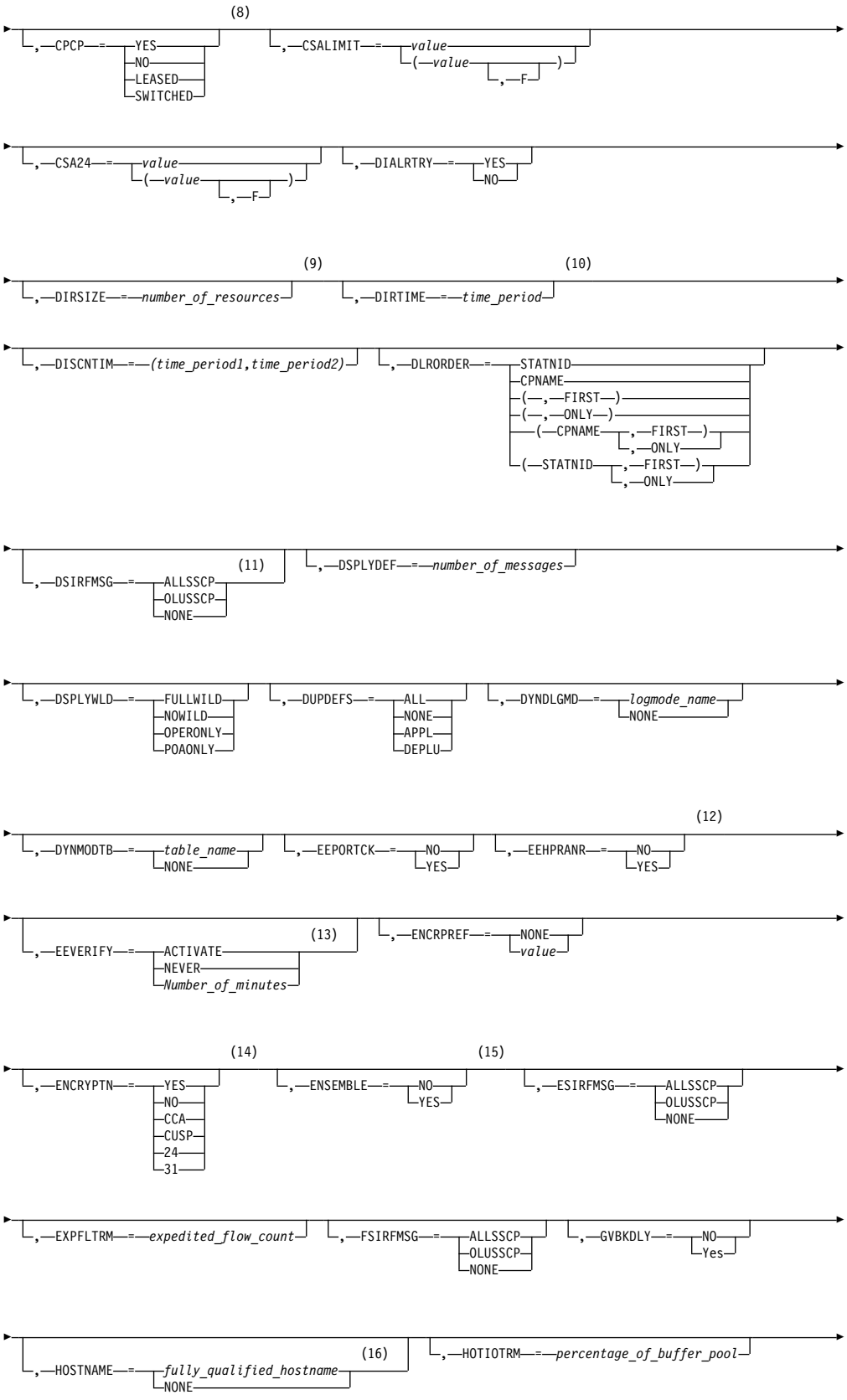
The NCP line trace and the transmission group trace are mutually exclusive for a particular line. Therefore, when starting a transmission group trace, select a line that is not being used, and is not likely to be used, for a line trace.

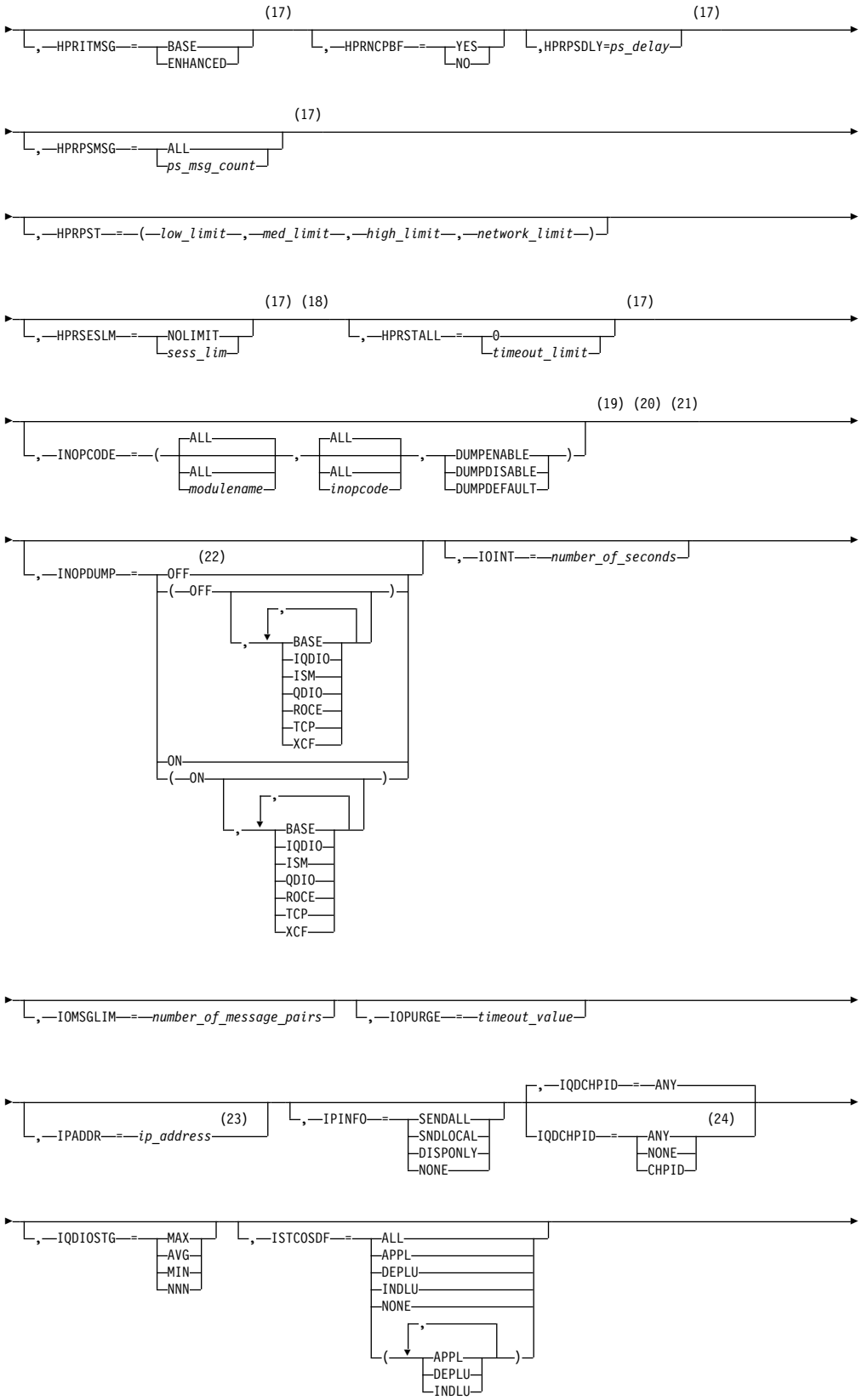
TYPE=TSO
Starts a TSO component trace for the user ID identified by the ID operand. GTF must be active when this trace option is specified.

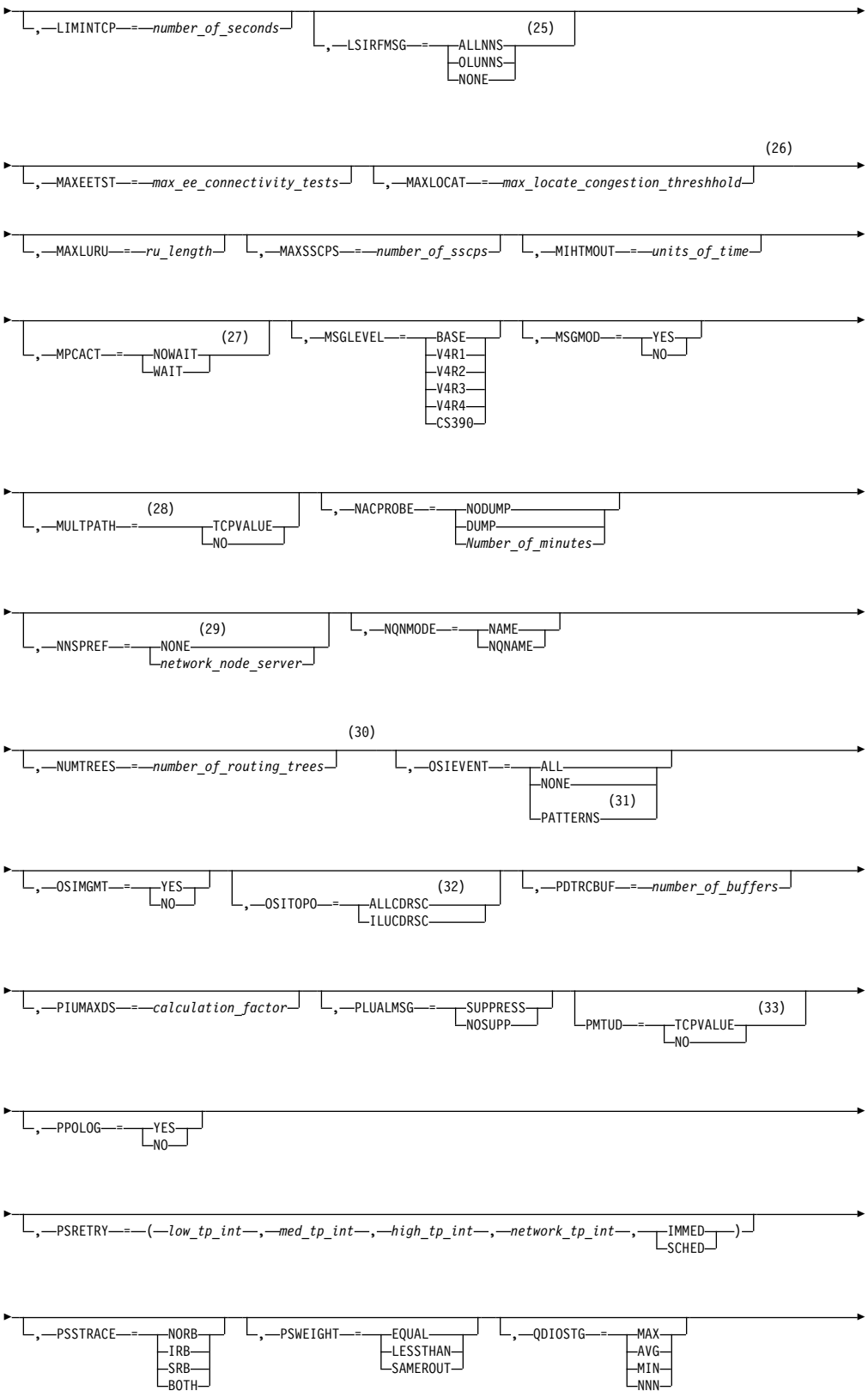
TYPE=VTAM
Starts the VTAM internal trace (VIT) for the components specified by the OPTION operand. If OPTION is omitted, no new component internal traces are initiated; rather, VTAM issues messages identifying the components for which the internal trace is currently active.

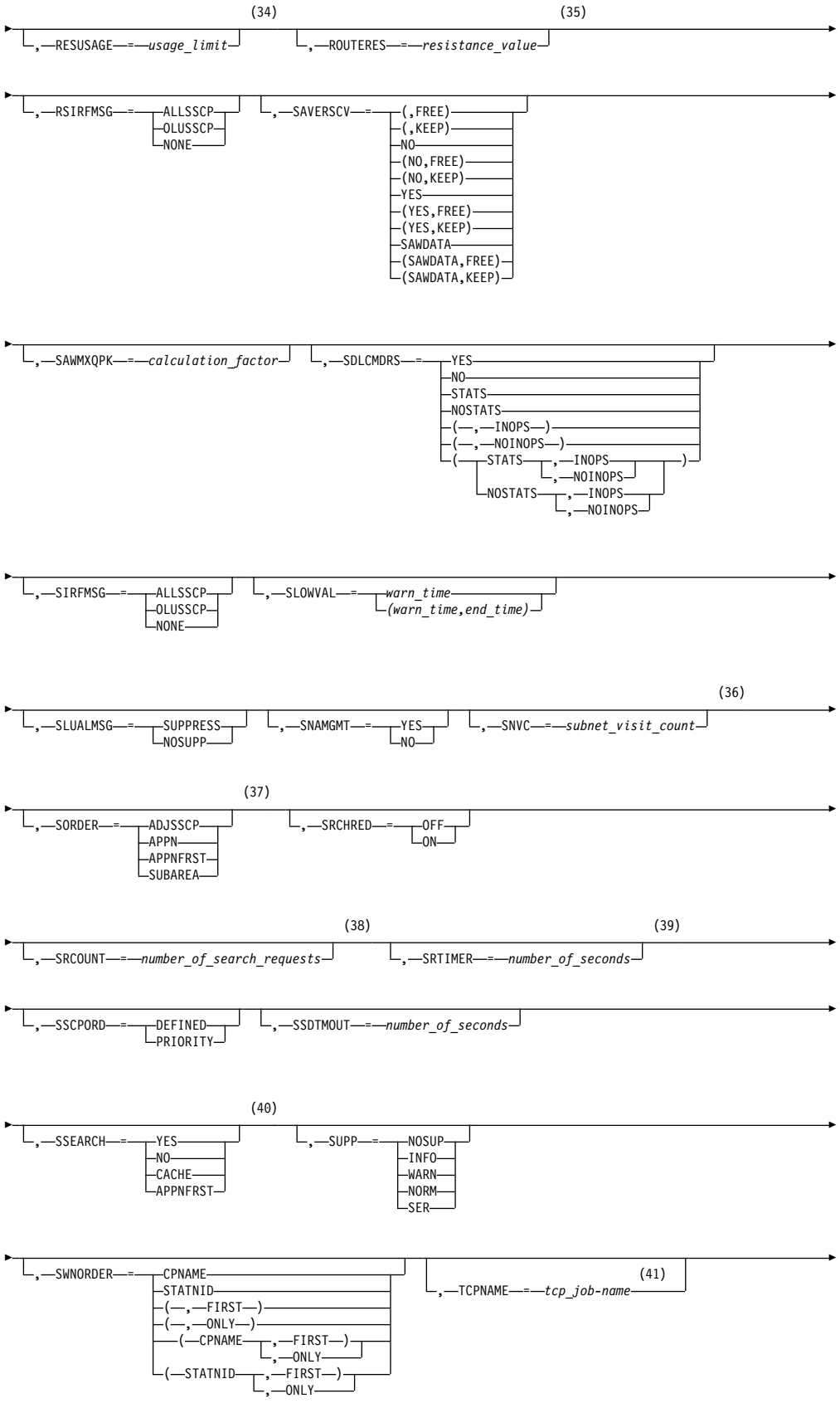
MODIFY VTAMOPTS command

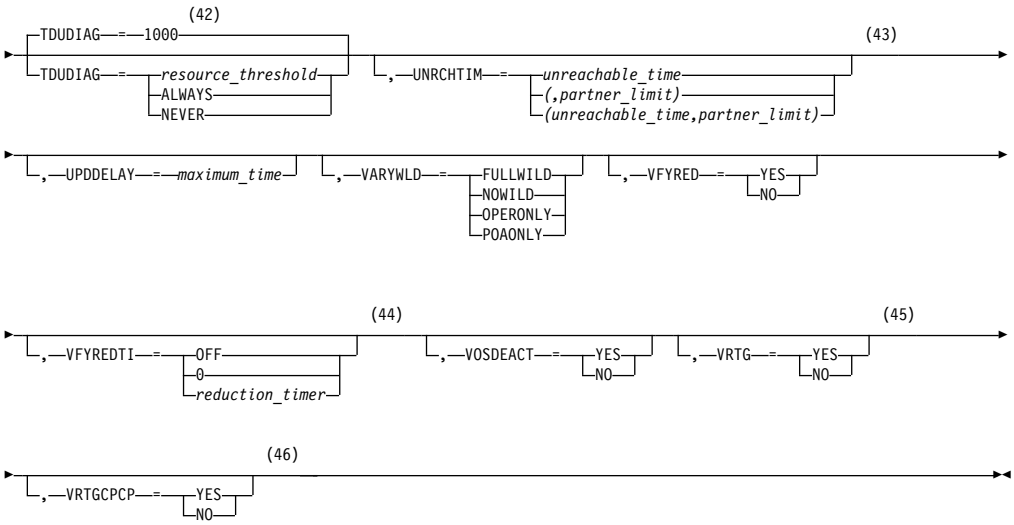



(8)
,—CPCP—=—YES
NO
LEASED
SWITCHED
,—CSALIMIT—=—value
(—value—,—F—)
,—CSA24—=—value
(—value—,—F—)
,—DIALRTRY—=—YES
NO
(9)
,—DIRSIZE—=—number_of_resources
(10)
,—DIRTIME—=—time_period
,—DISCNTIM—=—(time_period1,time_period2)
,—DLRORDER—=—STATNID
CPNAME
(—,—FIRST—)
(—,—ONLY—)
(—CPNAME—,—FIRST—)
,—ONLY
(—STATNID—,—FIRST—)
,—ONLY
(11)
,—DSIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—DSPLYDEF—=—number_of_messages
,—DSPLYWLD—=—FULLWILD
NOWILD
OPERONLY
POAONLY
,—DUPDEFS—=—ALL
NONE
APPL
DEPLU
,—DYNDLGMD—=—logmode_name
NONE
(12)
,—DYNMODTB—=—table_name
NONE
,—EEPORTCK—=—NO
YES
,—EEHPRANR—=—NO
YES
(13)
,—EEVERIFY—=—ACTIVATE
NEVER
Number_of_minutes
,—ENCRPREF—=—NONE
value
(14)
,—ENCRYPTN—=—YES
NO
CCA
CUSP
24
31
(15)
,—ENSEMBLE—=—NO
YES
,—ESIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—EXPFLTRM—=—expedited_flow_count
,—FSIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—GVBKDLY—=—NO
Yes
(16)
,—HOSTNAME—=—fully_qualified_hostname
NONE
,—HOTIOTRM—=—percentage_of_buffer_pool


(17)
,HPRITMSG=BASE
ENHANCED
,HPRNCPBF=YES
NO
(17)
,HPRPSDLY=ps_delay
(17)
,HPRPSMSG=ALL
ps_msg_count
,HPRPST=(low_limit,med_limit,high_limit,network_limit)
(17) (18)
,HPRSESLM=NOLIMIT
sess_lim
(17)
,HPRSTALL=0
timeout_limit
(19) (20) (21)
,INOPCODE=(ALL
ALL
modulename
,ALL
ALL
inopcode
,DUMPENABLE
DUMPDISABLE
DUMPDEFAULT)
,INOPDUMP=(22)
OFF
(OFF)
BASE
IQDIO
ISM
QDIO
ROCE
TCP
XCF
ON
(ON)
BASE
IQDIO
ISM
QDIO
ROCE
TCP
XCF
,IOINT=number_of_seconds
,IOMSGLIM=number_of_message_pairs
,IOPURGE=timeout_value
,IPADDR=ip_address
(23)
,IPINFO=SENDALL
SNDLOCAL
DISPONLY
NONE
,IQDCHPID=ANY
IQDCHPID=ANY
NONE
CHPID
(24)
,IQDIOSTG=MAX
AVG
MIN
NNN
,ISTCOSDF=ALL
APPL
DEPLU
INDLU
NONE
(APPL
DEPLU
INDLU)


,—LIMINTCP—=—number_of_seconds—
,—LSIRFMSG—=—(25)—ALLNNS—OLUNNS—NONE—
(26)
,—MAXEETST—=—max_ee_connectivity_tests—
,—MAXLOCAT—=—max_locate_congestion_threshhold—
,—MAXLURU—=—ru_length—
,—MAXSSCPS—=—number_of_sscps—
,—MIHTMOUT—=—units_of_time—
,—MPCACT—=—(27)—NOWAIT—WAIT—
,—MSGLEVEL—=—BASE—V4R1—V4R2—V4R3—V4R4—CS390—
,—MSGMOD—=—YES—NO—
,—MULTPATH—=—(28)—TCPVALUE—NO—
,—NACPROBE—=—NODUMP—DUMP—Number_of_minutes—
,—NNSPREF—=—(29)—NONE—network_node_server—
,—NQNMODE—=—NAME—NQNAME—
(30)
,—NUMTREES—=—number_of_routing_trees—
,—OSIEVENT—=—ALL—NONE—(31)—PATTERNS—
,—OSIMGMT—=—YES—NO—
,—OSITOPO—=—(32)—ALLCDRSC—ILUCDRSC—
,—PDTRCBUF—=—number_of_buffers—
,—PIUMAXDS—=—calculation_factor—
,—PLUALMSG—=—SUPPRESS—NOSUPP—
PMTUD—=—(33)—TCPVALUE—NO—
,—PPOLOG—=—YES—NO—
,—PSRETRY—=—(—low_tp_int—,—med_tp_int—,—high_tp_int—,—network_tp_int—,—IMMED—SCHED—)—
,—PSSTRACE—=—NORB—IRB—SRB—BOTH—
,—PSWEIGHT—=—EQUAL—LESSTHAN—SAMEROUT—
,—QDIOSTG—=—MAX—AVG—MIN—NNN—


(34)
(35)
,—RESUSAGE—=—usage_limit
,—ROUTERES—=—resistance_value
,—RSIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—SAVERSCV—=—(,FREE)
(,KEEP)
NO
(NO,FREE)
(NO,KEEP)
YES
(YES,FREE)
(YES,KEEP)
SAWDATA
(SAWDATA,FREE)
(SAWDATA,KEEP)
,—SAWMXQPK—=—calculation_factor
,—SDLCMDRS—=—YES
NO
STATS
NOSTATS
(—,—INOPS—)
(—,—NOINOPS—)
(—STATS—,—INOPS
,—NOINOPS
)
NOSTATS—,—INOPS
,—NOINOPS
,—SIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—SLOWVAL—=—warn_time
(warn_time,end_time)
(36)
,—SLUALMSG—=—SUPPRESS
NOSUPP
,—SNAMGMT—=—YES
NO
,—SNVC—=—subnet_visit_count
(37)
,—SORDER—=—ADJSSCP
APPN
APPNFRST
SUBAREA
,—SRCHRED—=—OFF
ON
(38)
(39)
,—SRCOUNT—=—number_of_search_requests
,—SRTIMER—=—number_of_seconds
,—SSCPORD—=—DEFINED
PRIORITY
,—SSDTMOUT—=—number_of_seconds
(40)
,—SSEARCH—=—YES
NO
CACHE
APPNFRST
,—SUPP—=—NOSUP
INFO
WARN
NORM
SER
,—SWNORDER—=—CPNAME
STATNID
(—,—FIRST—)
(—,—ONLY—)
(—CPNAME—,—FIRST—)
,—ONLY
(—STATNID—,—FIRST—)
,—ONLY
(41)
,—TCPNAME—=—tcp_job-name



Notes:

1 API64R can be modified only when running in z/Architecture® mode.

2 APPNCOS can be modified only if NODETYPE was specified during VTAM START processing.

3 BNDYN can be modified only if BN=YES was specified during VTAM START processing.

4 BNORD can be modified only if BN=YES was specified during VTAM START processing.

5 CDSREFER can be modified only if NODETYPE=NN and CDSERVR=NO were specified during VTAM START processing.

6 CMPMIPS is meaningful only if the value for CMPVTAM is greater than 1.

7 CONNTYPE can be modified only if NODETYPE was specified during VTAM START processing.

8 CPCP can be modified only if NODETYPE was specified during VTAM START processing.

9 DIRSIZE can be modified only if NODETYPE=NN was specified during VTAM START processing.

10 DIRTIME can be modified only if NODETYPE=NN was specified during VTAM START processing.

11 Because of the volume of messages that can be generated, it is not recommended that this option be enabled during normal operation. Instead, it is recommended that this option be enabled (using the MODIFY VTAMOPTS command) on all necessary hosts only when trying to diagnose specific problems. After the problem has been diagnosed or documentation has been collected, this option should be disabled once again (using the MODIFY VTAMOPTS command).

12 EEHPRANR is meaningful only when the NODETYPE=NN start option is also used.

13 The EEVERIFY start option is meaningful only if VTAM provides RTP-level

HPR support. The EEVERIFY start option can be modified only if the NODETYPE start option is specified and the RTP value is specified on the HPR start option.

14 The ENCRYPTN start option cannot be modified if ENCRYPTN=NO was specified during VTAM START processing.

15 The ENSEMBLE setting is used to either permit or deny connectivity to the intraensemble data network and the intranode management network. The ensemble setting permits or denies connectivity by either allowing or denying activation of OSX and OSM interfaces. Modifying the ENSEMBLE start option does not cause z/OS Communications Server to take action on active OSX or OSM interfaces.

16 HOSTNAME can be modified only if NODETYPE was specified during VTAM START processing. Displays of VTAM start options will show the new value immediately; however, the new value will not be used until all Enterprise Extender lines, whose GROUP definition statements do not have HOSTNAME explicitly coded, are inactive. Any subsequent line activation from the Enterprise Extender XCA major node, whose GROUP definition statements do not have HOSTNAME explicitly coded, will make use of the new HOSTNAME start option value. The IPADDR start option, if it is in effect at the time when the MODIFY VTAMOPTS,HOSTNAME=*hostname* is specified, will be reset (that is, set to a value of 0.0.0.0) as part of the MODIFY processing. The value NONE can be used to clear the setting of the HOSTNAME start option. HOSTNAME and IPADDR cannot be modified using one MODIFY VTAMOPTS command. If both start options are specified on the same MODIFY command, they will both be ignored and message IST1917I will be generated.

17 This option is meaningful only if VTAM provides RTP-level HPR support.

18 If the current value of the HPRSESLM start option is DISABLED, then the HPRSESLM value can be changed only by stopping and restarting VTAM.

19 When specifying an InOpCode for the second parameter, always specify three digits by including any leading zeros.

20 If an InOpCode is specified for the second parameter, the first parameter cannot be ALL.

21 INOPCODE has no effect unless INOPDUMP is active for the resource when an inoperative condition is detected. See the section called MODIFY INOPCODE command for more details.

22 When altering the INOPDUMP VTAM start option, the resulting INOPDUMP status is propagated to all TRLEs in the TRL major node if the command is globally set, or it is propogated to a subset of resources that are identified by one or more INOPDUMP control groups. The INOPDUMP setting becomes the default status for any subsequently activated TRLEs.

23 IPADDR can be modified only if NODETYPE was specified during VTAM START processing. The new value will not be used until all lines, defined with or defaulting to the old value of the IPADDR start option, in the XCA major node used for Enterprise Extender are inactive. However, displays of VTAM start options will show the new value immediately. Any subsequent line activation from the Enterprise Extender XCA major node, whose GROUP definition statement does not specify the IPADDR operand, will make use of the new IPADDR start option value. The HOSTNAME start option, if it is in effect at the time when the MODIFY VTAMOPTS,IPADDR=*ip_address* is specified, will be reset (that is, set to a value of NONE) as part of the

MODIFY processing. The value of 0.0.0.0, or an IPv6 address of all zeros, usually written as ::, can be used to clear the setting of the IPADDR start option. HOSTNAME and IPADDR cannot be modified using one MODIFY VTAMOPTS command. If both start options are specified on the same MODIFY command, they will both be ignored and message IST1917I will be generated.

24 The IQDCHPID option controls which IQD CHPID (and related subchannel devices) VTAM selects to dynamically build the iQDIO (IUTIQDIO) MPC group. The IUTIQDIO MPC group is used for TCP/IP dynamic XCF communications within System z. Although this option can be modified (and the modification will immediately be displayed) while the IUTIQDIO MPC group is currently active, any modifications have the effects shown in the section called IQD CHPID modifications.

25 Because of the volume of messages that can be generated, it is not recommended that this option be enabled during normal operation. Instead, it is recommended that this option be enabled (using the MODIFY VTAMOPTS command) on all necessary hosts only when trying to diagnose specific problems. After the problem has been diagnosed or documentation has been collected, this option should be disabled once again (using the MODIFY VTAMOPTS command).

26 MAXLOCAT can be modified only if NODETYPE was specified during VTAM START processing.

27 The option does not take effect for MPC groups that are in the process of being activated when the command is issued until those MPC groups are deactivated and reactivated.

28 MULTPATH is meaningful only if the NODETYPE start option is also specified.

29 NNSPREF can be modified only if NODETYPE=EN was specified during VTAM START processing.

30 NUMTREES can be modified only if NODETYPE=NN was specified during VTAM START processing.

31 OSIEVENT=PATTERNS is not valid when OSIMGMT=YES.

32 OSITOPO=ALLCDRSC is not valid when OSIMGMT=YES.

33 PMTUD is meaningful only if the NODETYPE start option is also specified.

34 RESUSAGE can be modified only if NODETYPE=NN was specified during VTAM START processing.

35 ROUTERES can be modified only if NODETYPE=NN was specified during VTAM START processing.

36 SNVC can be modified only if BN=YES was specified during VTAM START processing.

37 SORDER can be modified only if VTAM has been started as an interchange node or a migration data host.

38 SRCOUNT is meaningful only when SRCHRED=ON.

39 SRTIMER is meaningful only when SRCHRED=ON.

40 SSEARCH can be modified only if NODETYPE=NN was specified during VTAM START processing.

41 TCPNAME can be modified only if NODETYPE was specified during VTAM

START processing. The new value will not be used until all lines in the XCA major node used for Enterprise Extender are inactive. However, displays of VTAM start options will show the new value immediately. Any subsequent line activation from the Enterprise Extender XCA major node will make use of the new TCPNAME value.

42 TDUDIAG is meaningful only if the NODETYPE=NN start option is also available.

43 UNRCHTIM is meaningful only if the NODETYPE start option is also used.

44 VFYREDTI can be modified only if NODETYPE=NN was specified during VTAM START processing.

45 VRTG can be modified only if NODETYPE and HOSTSA are specified.

46 VRTGCPCP can be modified only if NODETYPE and HOSTSA are specified.

Abbreviations

Operand	Abbreviation
MODIFY	F
MSGLEVEL	MSGLVL
PLUALMSG=NOSUPP	PLUALMSG=NOSUP
PLUALMSG=SUPPRESS	PLUALMSG=SUPP
SLUALMSG=NOSUPP	SLUALMSG=NOSUP
SLUALMSG=SUPPRESS	SLUALMSG=SUPP

When using an abbreviation in place of an operand, code the abbreviation exactly as shown in the table. For example, when coding the abbreviation for PLUALMSG=SUPPRESS, code only PLUALMSG=SUPP.

Purpose

The MODIFY VTAMOPTS (VTAM start options) command enables you to change certain values that might have been specified on VTAM start options. See the z/OS Communications Server: SNA Resource Definition Reference for descriptions of each of the start options that you can change with this command.

There are no default values on the MODIFY VTAMOPTS command. In general, only the values that you specify are affected, and operands that are not specified on the command are unaffected. The exceptions are the IPADDR and HOSTNAME operands, which do affect each other when specified on the MODIFY VTAMOPTS command.

Note: If a start option affects individual resources, and you change the value of the start option with this command, the change does not go into effect until the major nodes for those resources are deactivated and reactivated. The command takes effect for major nodes that are activated after you issue this command and for dynamic cross-network resources that are dynamically defined after the command is issued.

Operands

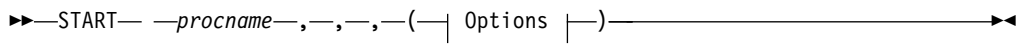
procname
The procedure name for the command. If *procname* in the START command

was specified as *startname.ident*, where *startname* is the VTAM start procedure and *ident* is the optional identifier, either *startname.ident* or *ident* can be specified for *procname*.

If *procname* in the START command was *startname*, *startname* must be specified for *procname*.

START command

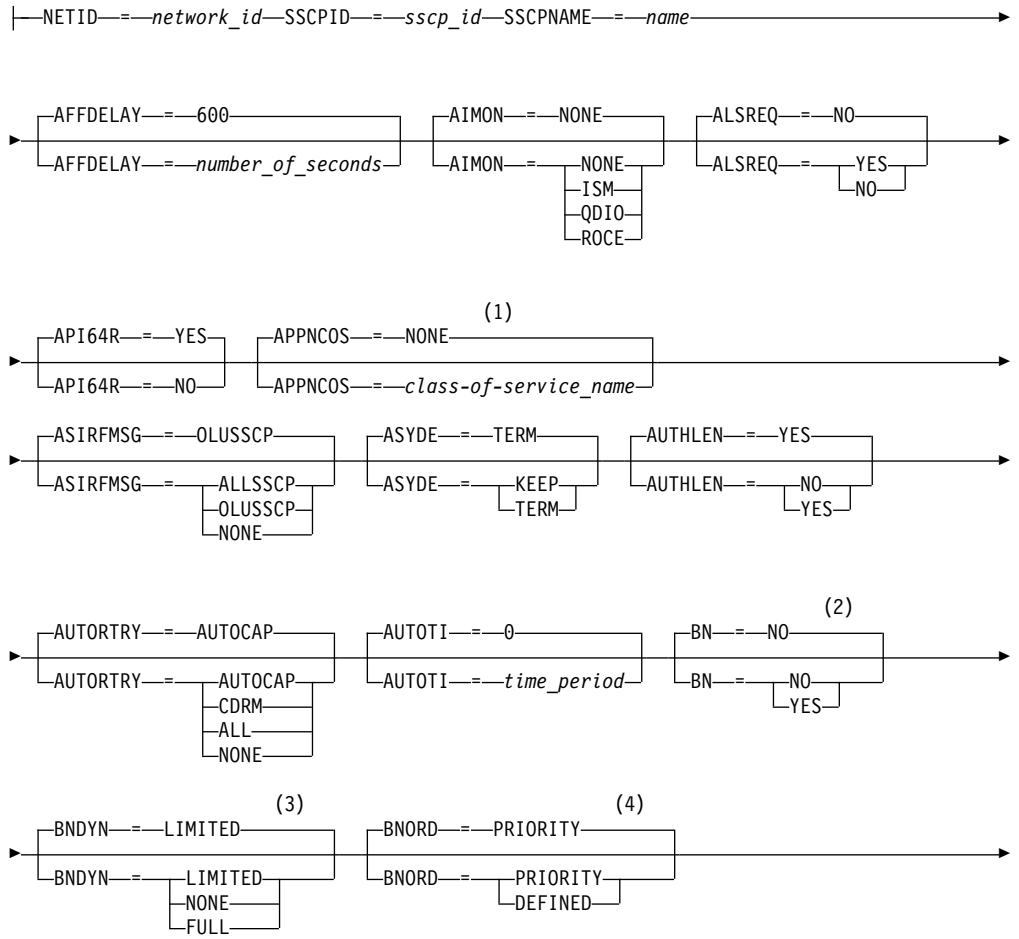
Starting VTAM in an MVS environment:

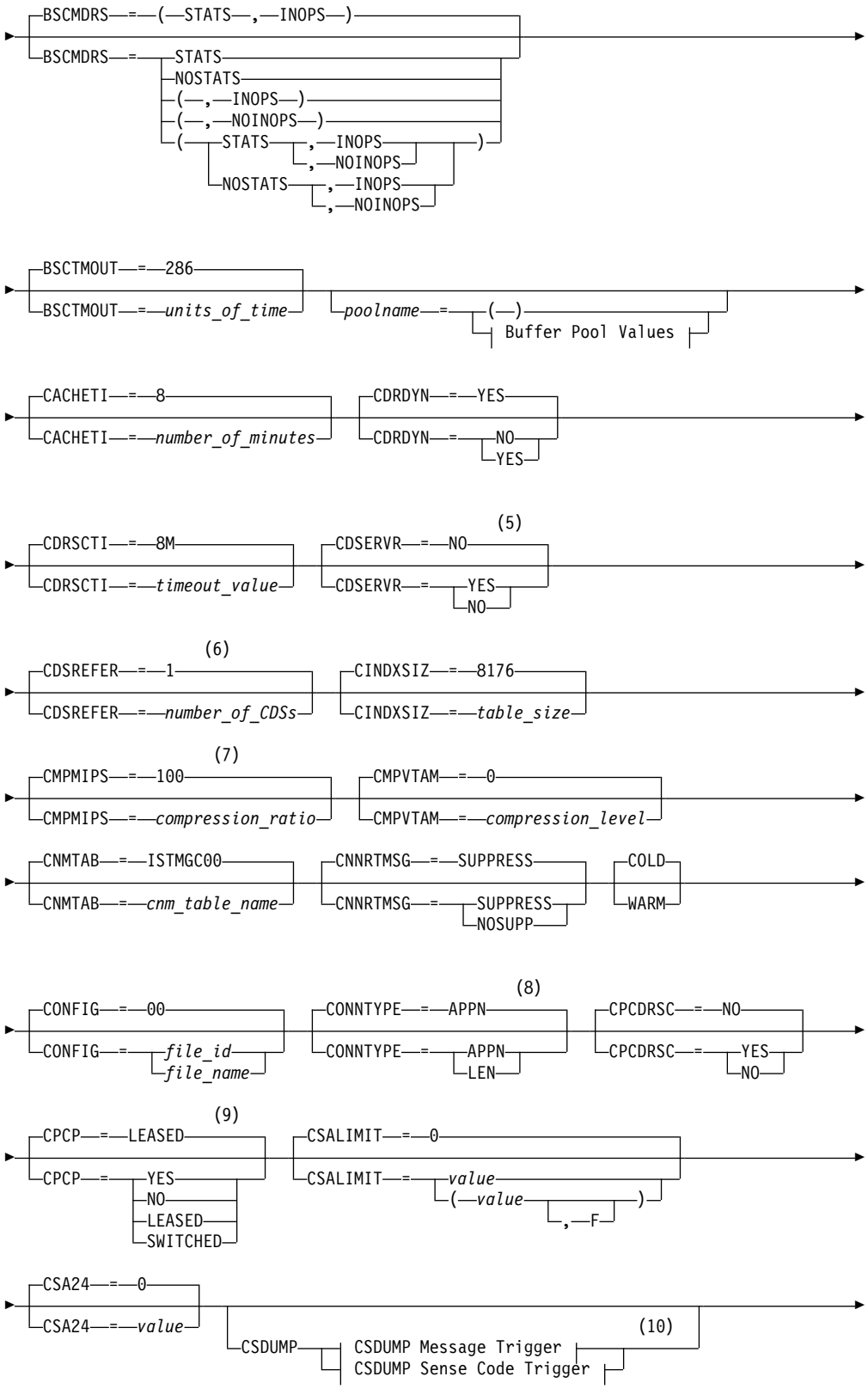


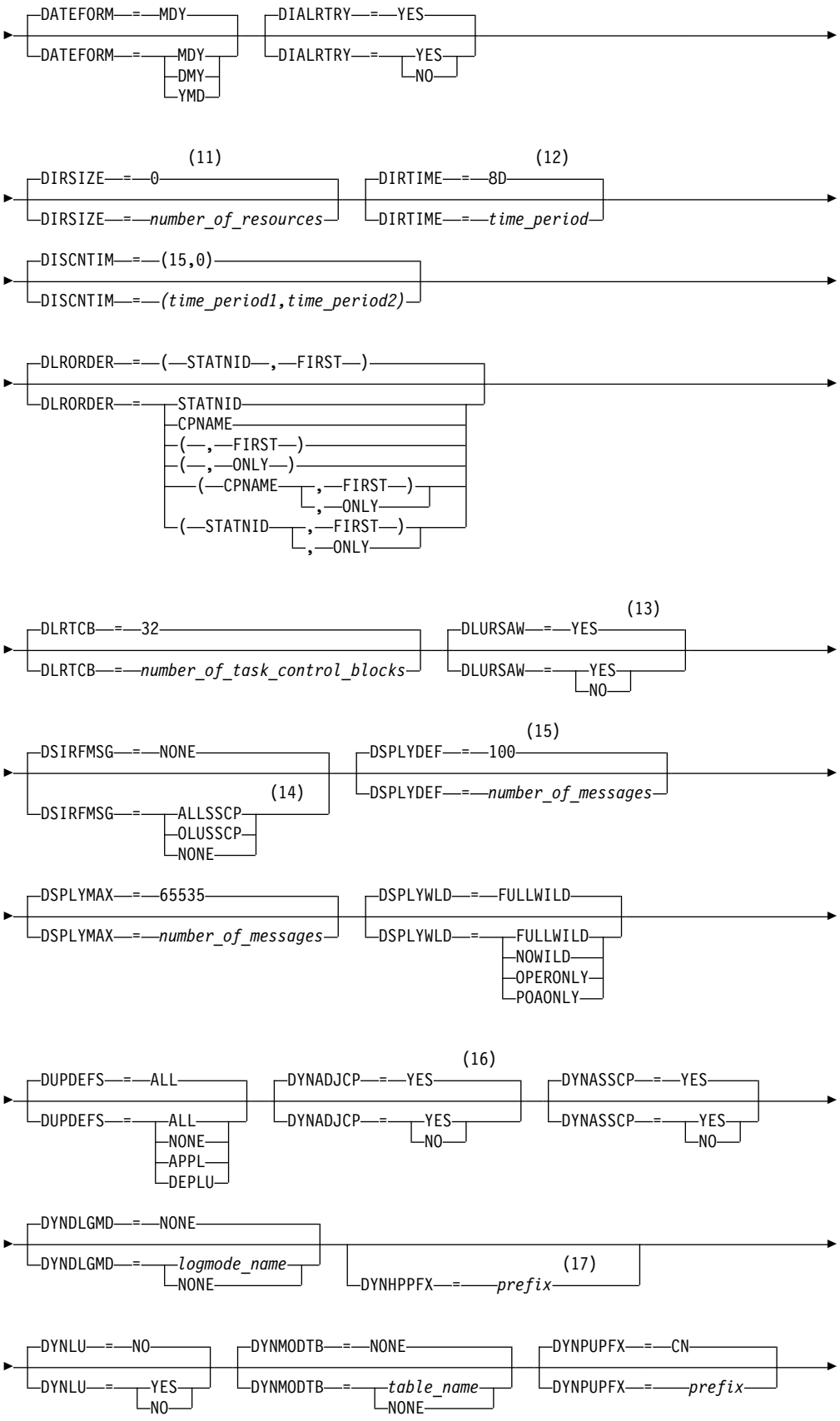
Note:

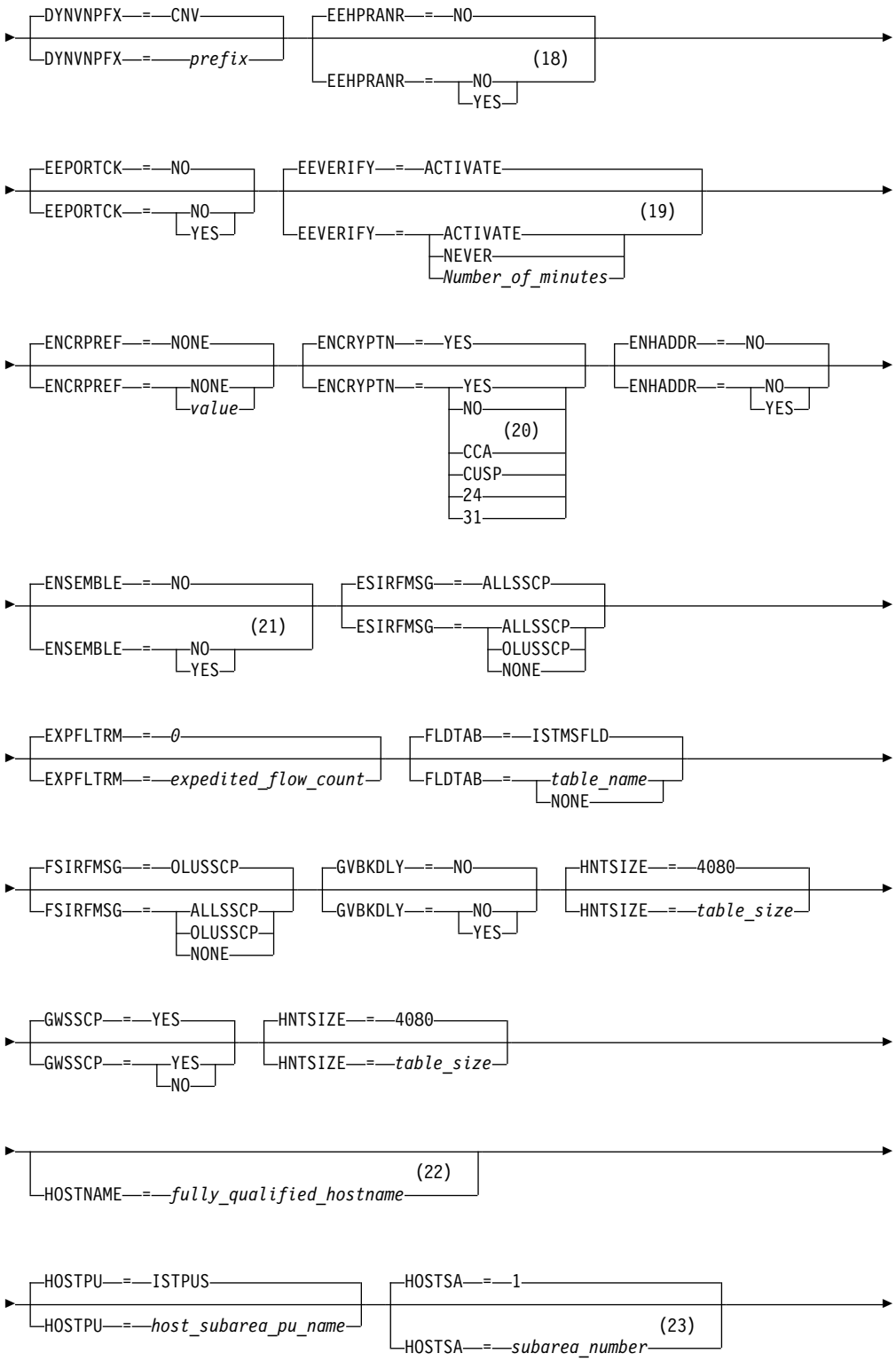
1. The start options are listed in this information alphabetically; however, you can code them in any order.
2. Precede the option list with three commas and enclose the group of options in parentheses.
3. Start options that are entered on the START command must be separated by commas. Do not leave any blanks between options.

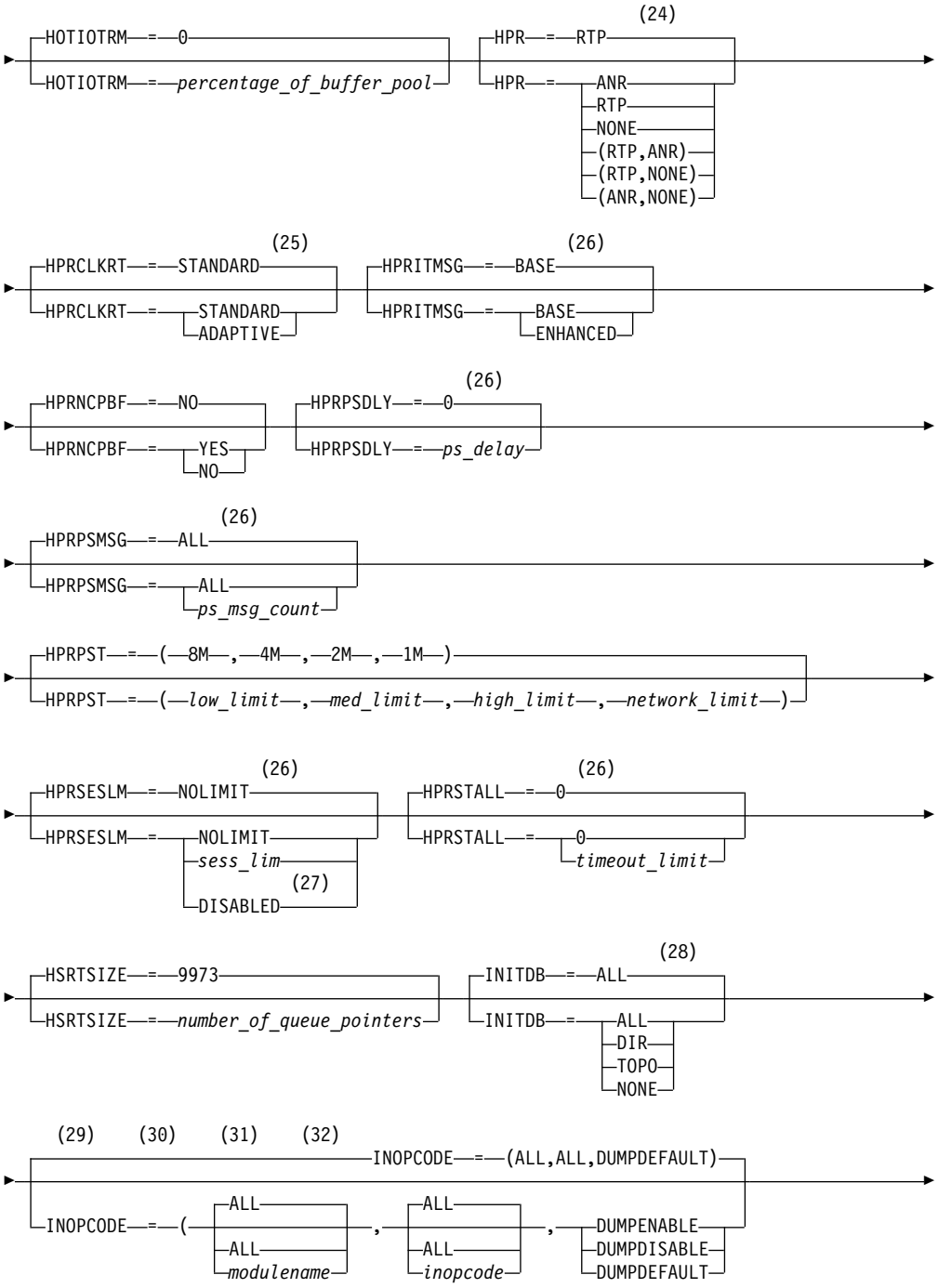
Options:

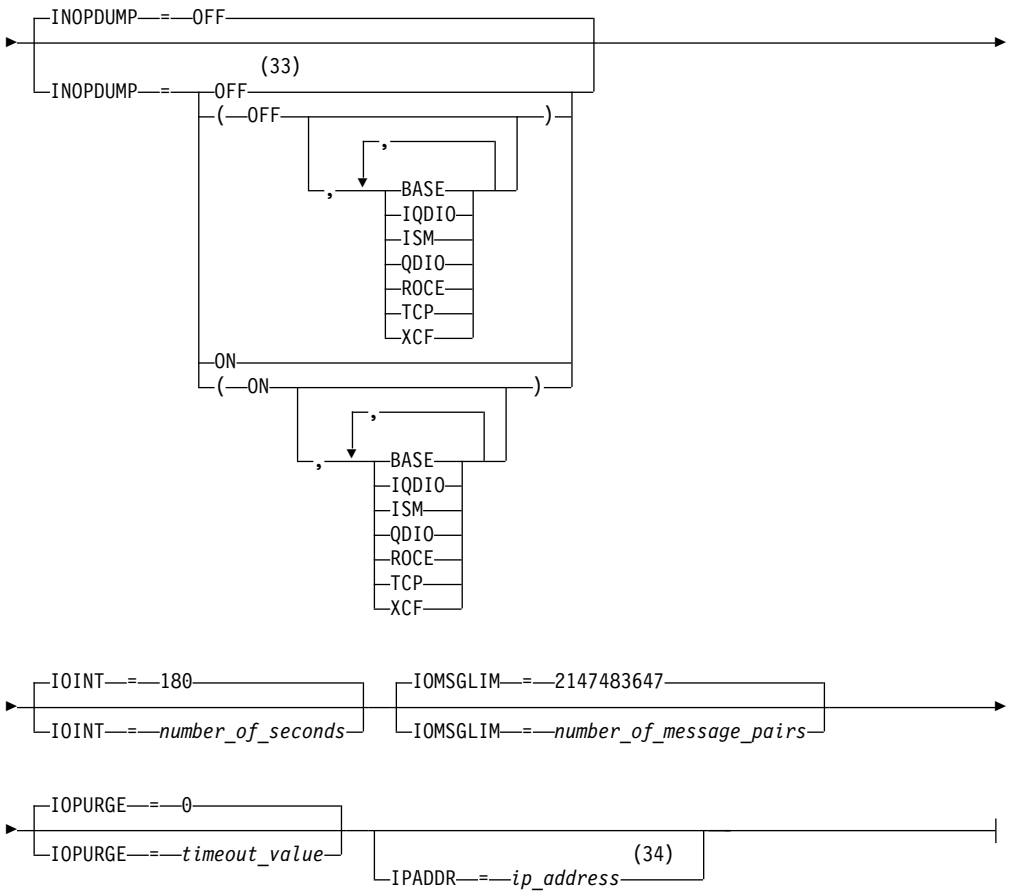



BSCMDRS=(STATS,INOPS)
BSCMDRS=STATS
NOSTATS
(,INOPS)
(,NOINOPS)
(STATS,INOPS)
,NOINOPS
NOSTATS,INOPS
,NOINOPS
BSCTMOUT=286
BSCTMOUT=units_of_time
poolname=(
Buffer Pool Values
CACHETI=8
CACHETI=number_of_minutes
CDRDYN=YES
CDRDYN=NO
YES
(5)
CDRSCTI=8M
CDRSCTI=timeout_value
CDSERVR=NO
CDSERVR=YES
NO
(6)
CDSREFER=1
CDSREFER=number_of_CDSs
CINDXSIZ=8176
CINDXSIZ=table_size
(7)
CMPMIPS=100
CMPMIPS=compression_ratio
CMPVTAM=0
CMPVTAM=compression_level
CNMTAB=ISTMGC00
CNMTAB=cnm_table_name
CNNRTMSG=SUPPRESS
CNNRTMSG=SUPPRESS
NOSUPP
COLD
WARM
(8)
CONFIG=00
CONFIG=file_id
file_name
CONNTYPE=APPN
CONNTYPE=APPN
LEN
CPCDRSC=NO
CPCDRSC=YES
NO
(9)
CPCP=LEASED
CPCP=YES
NO
LEASED
SWITCHED
CSALIMIT=0
CSALIMIT=value
(value,F)
CSA24=0
CSA24=value
CSDUMP
CSDUMP Message Trigger
CSDUMP Sense Code Trigger
(10)


DATEFORM
MDY
DMY
YMD
DIALRTRY
YES
NO
(11)
DIRSIZE
0
number_of_resources
(12)
DIRTIME
8D
time_period
DISCNTIM
(15,0)
(time_period1,time_period2)
DLRORDER
(STATNID,FIRST)
STATNID
CPNAME
(,FIRST)
(,ONLY)
(CPNAME
,FIRST)
,ONLY)
(STATNID
,FIRST)
,ONLY)
DLRTCB
32
number_of_task_control_blocks
(13)
DLURSAW
YES
NO
DSIRFMSG
NONE
(14)
ALLSSCP
OLUSSCP
NONE
(15)
DSPLYDEF
100
number_of_messages
DSPLYMAX
65535
number_of_messages
DSPLYWLD
FULLWILD
NOWILD
OPERONLY
POAONLY
DUPDEFS
ALL
NONE
APPL
DEPLU
(16)
DYNADJCP
YES
NO
DYNASSCP
YES
NO
DYNDLGMD
NONE
logmode_name
DYNHPPFX
(17)
prefix
DYNLU
NO
YES
DYNMODTB
NONE
table_name
DYNPUPFX
CN
prefix


DYNVNPFX=CNV
DYNVNPFX=prefix
EEHPRANR=NO
EEHPRANR=NO
YES
(18)
EEPORTCK=NO
EEPORTCK=NO
YES
EEVERIFY=ACTIVATE
EEVERIFY=ACTIVATE
NEVER
Number_of_minutes
(19)
ENCRPREF=NONE
ENCRPREF=NONE
value
ENCRYPTN=YES
ENCRYPTN=YES
NO
CCA
CUSP
24
31
(20)
ENHADDR=NO
ENHADDR=NO
YES
ENSEMBLE=NO
ENSEMBLE=NO
YES
(21)
ESIRFMSG=ALLSSCP
ESIRFMSG=ALLSSCP
OLUSSCP
NONE
EXPFLTRM=0
EXPFLTRM=expedited_flow_count
FLDTAB=ISTMSFLD
FLDTAB=table_name
NONE
FSIRFMSG=OLUSSCP
FSIRFMSG=ALLSSCP
OLUSSCP
NONE
GVBKDLY=NO
GVBKDLY=NO
YES
HNTSIZE=4080
HNTSIZE=table_size
GWSSCP=YES
GWSSCP=YES
NO
HNTSIZE=4080
HNTSIZE=table_size
HOSTNAME=fully_qualified_hostname
(22)
HOSTPU=ISTPUS
HOSTPU=host_subarea_pu_name
HOSTSA=1
HOSTSA=subarea_number
(23)


HOTIOTRM = 0
HOTIOTRM = percentage_of_buffer_pool
(24)
HPR = RTP
HPR = ANR
RTP
NONE
(RTP,ANR)
(RTP,NONE)
(ANR,NONE)
(25)
HPRCLKRT = STANDARD
HPRCLKRT = STANDARD
ADAPTIVE
(26)
HPRITMSG = BASE
HPRITMSG = BASE
ENHANCED
HPRNCPBF = NO
HPRNCPBF = YES
NO
(26)
HPRPSDLY = 0
HPRPSDLY = ps_delay
(26)
HPRPSMSG = ALL
HPRPSMSG = ALL
ps_msg_count
HPRPST = (8M , 4M , 2M , 1M)
HPRPST = (low_limit , med_limit , high_limit , network_limit)
(26)
HPRSESLM = NOLIMIT
HPRSESLM = NOLIMIT
sess_lim
(27)
DISABLED
(26)
HPRSTALL = 0
HPRSTALL = 0
timeout_limit
HSRTSIZE = 9973
HSRTSIZE = number_of_queue_pointers
(28)
INITDB = ALL
INITDB = ALL
DIR
TOPO
NONE
(29) (30) (31) (32)
INOPCODE = (ALL,ALL,DUMPDEFAULT)
INOPCODE = (ALL , ALL , DUMPENABLE
ALL
modulename
ALL
inopcode
DUMPDISABLE
DUMPDEFAULT



Notes:

1 APPNCOS is meaningful only if the NODETYPE start option is also used.

2 BN is meaningful only if the NODETYPE=NN start option is also used.

3 BNDYN is meaningful only if the BN=YES start option is also used.

4 BNORD is meaningful only if the BN=YES start option is also used.

5 CDSERVR is meaningful only if the NODETYPE=NN start option is also used.

6 CDSREFER is meaningful only if the NODETYPE=NN and CDSERVR=NO start options are also used.

7 The CMPMIPS start option is meaningful only if the value for CMPVTAM is greater than 1.

8 CONNTYPE is meaningful only if the NODETYPE start option is also used.

9 CPCP is meaningful only if the NODETYPE start option is also used.

10 Specify the CSDUMP start option twice to set both message and sense code triggers.

11 DIRSIZE is meaningful only if the NODETYPE=NN start option is also used.

12 DIRTIME is meaningful only if the NODETYPE=NN start option is also used.

13 DLURSAW is meaningful only if the NODETYPE=NN start option is also used.

14 Because of the volume of messages that can be generated, it is not recommended that this option be enabled during normal operation. Instead, it is recommended that this option be enabled (using the MODIFY VTAMOPTS command) on all necessary hosts only when trying to diagnose specific problems. After the problem has been diagnosed or documentation has been collected, this option should be disabled once again (using the MODIFY VTAMOPTS command).

15 If the DSPLYMAX start option value is less than 100, that value is the default for DSPLYDEF.

16 DYNADJCP is meaningful only if the NODETYPE start option is also used.

17 Two character prefix.

18 EEHPRANR is meaningful only when the NODETYPE=NN start option is also used.

19 The EEVERIFY start option is meaningful only if VTAM provides RTP-level HPR support. The NODETYPE start option must be coded and the RTP value must be specified on the HPR start option.

20 ENCRYPTN=CCA needs to be coded when Triple Des Encryption is required.

21 The ENSEMBLE setting is used to either permit or deny connectivity to the intraensemble data network and the intranode management network. It does this by either allowing or denying activation of OSX and OSM interfaces.

22 HOSTNAME is meaningful only if the NODETYPE start option is also used. If neither HOSTNAME nor IPADDR is specified on any of the GROUP definition statements within the Enterprise Extender XCA major node, then either the HOSTNAME, TCPNAME, or IPADDR start options must be specified in order to activate an Enterprise Extender link. The HOSTNAME start option specifies the default hostname to be used for name-to-address resolution as part of activating an Enterprise Extender connection, and must resolve at this node to a static VIPA address associated with a TCP/IP stack at this node. If IPADDR is specified along with HOSTNAME on the START command, the IPADDR value is ignored.

23 HOSTSA specifies the subarea number of this VTAM. If HOSTSA is not coded, then a default subarea number of 1 is used.

24 HPR is meaningful only if NODETYPE is also used.

25 HPRCLKRT=ADAPTIVE is meaningful only in Enterprise Extender configurations that have a defined capacity of 1 Gb (gigabit) or higher access speeds.

26 This option is meaningful only if VTAM provides RTP-level HPR support.

27 HPRSESLM=DISABLED is meaningful only on interchange nodes.

28 INITDB is meaningful only if the NODETYPE=NN start option is also used.

29 When specifying an InOpCode for the second parameter, always specify three digits by including any leading zeros.

30 If an InOpCode is specified for the second parameter, the first parameter cannot be ALL.

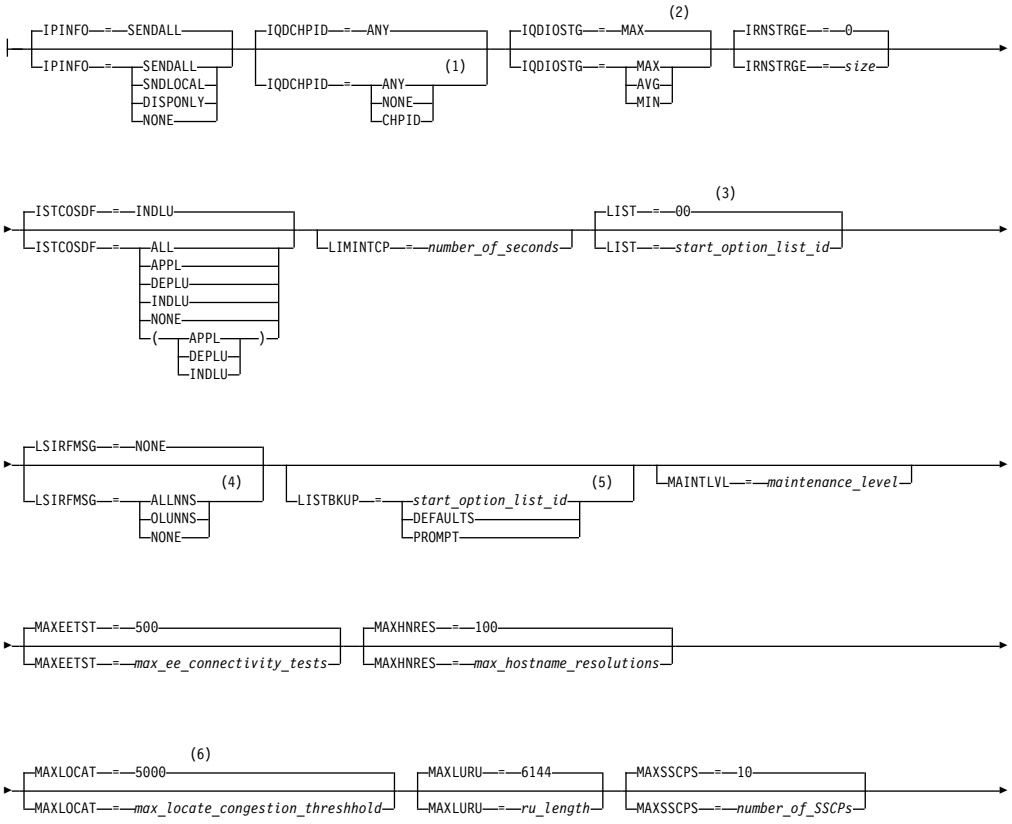
31 INOPCODE has no effect unless INOPDUMP is active for the resource when an inoperative condition is detected. See the MODIFY INOPCODE command for more details.

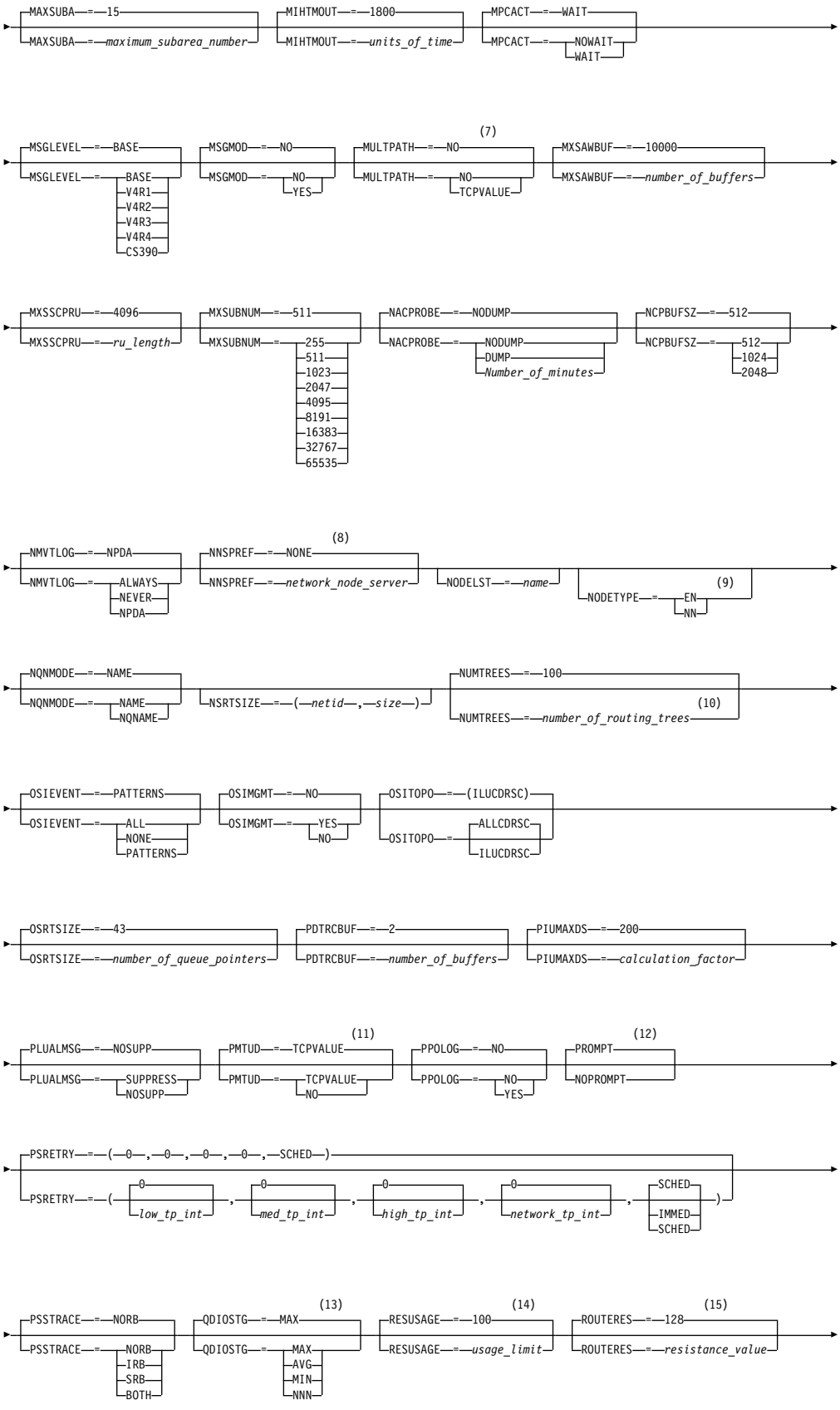
32 Multiple INOPCODE parameters can be specified by the START command,

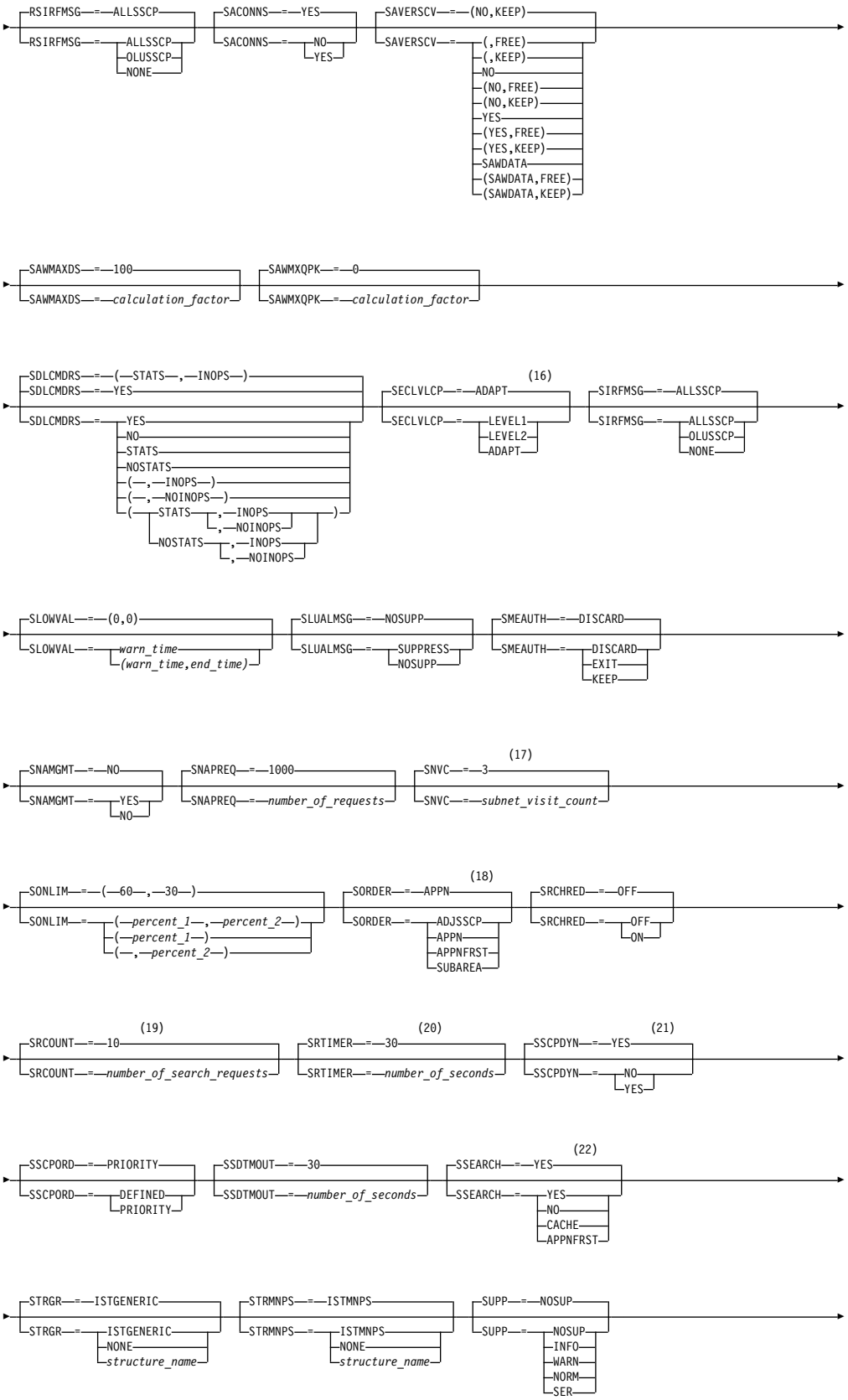
and will be processed left to right as they are entered. This is different from specifying the INOPCODE parameter on either the MODIFY INOPCODE command or the MODIFY VTAMOPTS command, where only one INOPCODE parameter is allowed for each entry of these commands.

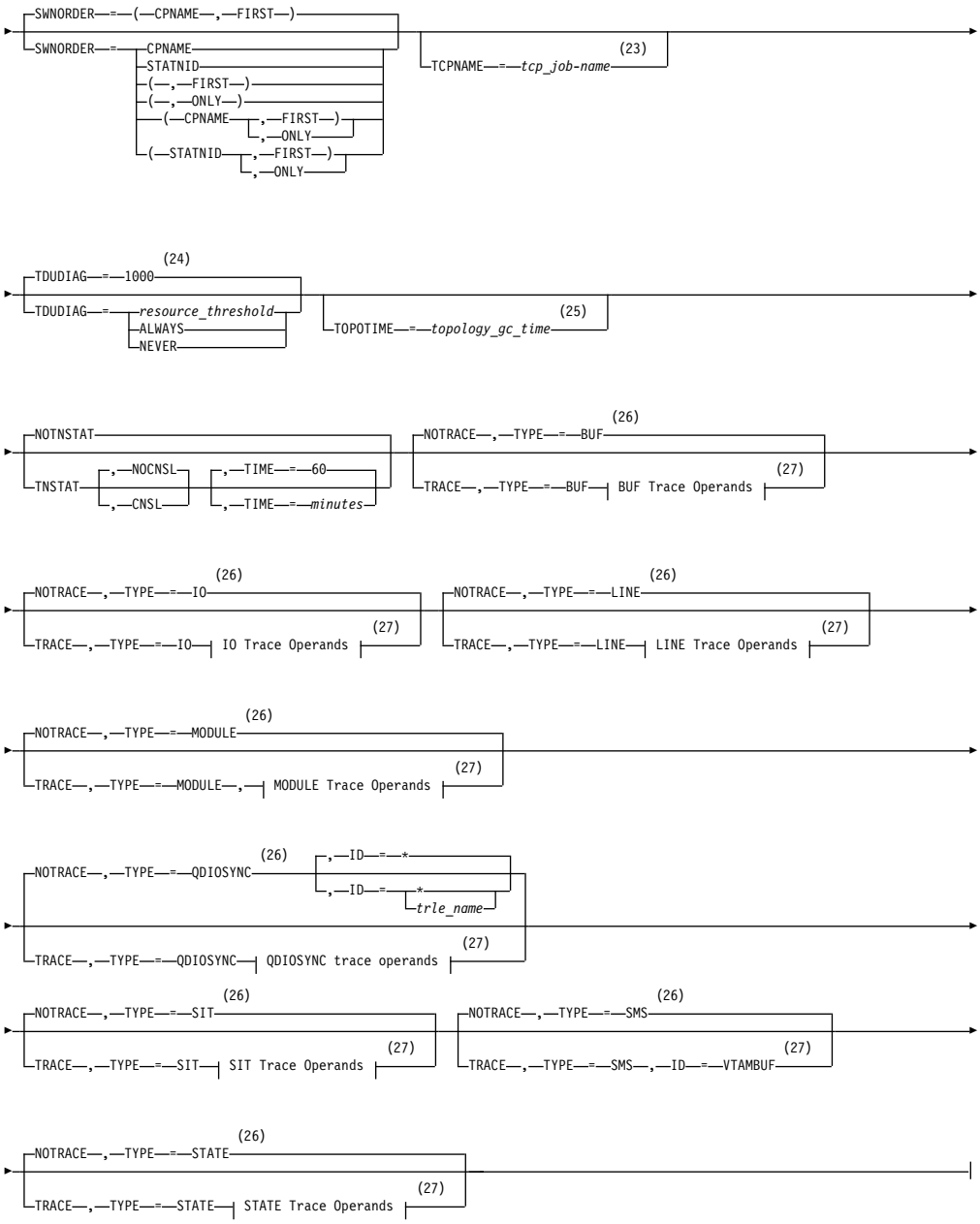
33 INOPDUMP status is propagated to resources that are defined within a TRLE when the entry is activated.

34 IPADDR is meaningful only if the NODETYPE start option is also used. If neither IPADDR nor HOSTNAME is specified on any of the GROUP definition statements within the Enterprise Extender XCA major node, then either the HOSTNAME, TCPNAME, or IPADDR start option must be specified in order to activate an Enterprise Extender link. The IPADDR start option specifies the default IPv4 or IPv6 static VIPA address to be used when activating an Enterprise Extender connection. If HOSTNAME is specified along with IPADDR on the START command, the IPADDR value is ignored.




MAXSUBA
15
maximum_subarea_number
MIHTMOUT
1800
units_of_time
MPCACT
WAIT
NOWAIT
WAIT
MSGLEVEL
BASE
V4R1
V4R2
V4R3
V4R4
CS390
MSGMOD
NO
YES
(7)
MULTPATH
NO
TCPVALUE
MXSAWBUF
10000
number_of_buffers
MXSSCPRU
4096
ru_length
MXSUBNUM
255
511
1023
2047
4095
8191
16383
32767
65535
NACPROBE
NODUMP
DUMP
Number_of_minutes
NCPBUFSZ
512
1024
2048
NMVTLOG
NPDA
ALWAYS
NEVER
NPDA
(8)
NNSPREF
NONE
network_node_server
NODELST
name
(9)
NODETYPE
EN
NN
NQNMODE
NAME
NQNAME
NSRTSIZE
netid
size
NUMTREES
100
(10)
number_of_routing_trees
OSIEVENT
PATTERNS
ALL
NONE
PATTERNS
OSIMGMT
NO
YES
OSITOPO
(ILUCDRSC)
ALLCDRSC
ILUCDRSC
OSRTSIZE
43
number_of_queue_pointers
PDTRCBUF
2
number_of_buffers
PIUMAXDS
200
calculation_factor
PLUALMSG
NOSUPP
SUPPRESS
NOSUPP
PMTUD
TCPVALUE
NO
(11)
PPOLOG
NO
YES
PROMPT
NOPROMPT
(12)
PSRETRY
(0,0,0,0,SCHED)
low_tp_int
med_tp_int
high_tp_int
network_tp_int
SCHED
IMMED
SCHED
PSSTRACE
NORB
IRB
SRB
BOTH
QDIOSTG
MAX
AVG
MIN
NNN
(13)
RESUSAGE
100
usage_limit
(14)
ROUTERES
128
resistance_value
(15)


RSIRFMSG
ALLSSCP
OLUSSCP
NONE
SACONNS
YES
NO
SAVERSCV
(NO,KEEP)
(,FREE)
(,KEEP)
NO
(NO,FREE)
(NO,KEEP)
YES
(YES,FREE)
(YES,KEEP)
SAWDATA
(SAWDATA,FREE)
(SAWDATA,KEEP)
SAWMAXDS
100
calculation_factor
SAWMXQPK
0
calculation_factor
SDLCMDRS
(STATS,INOPS)
YES
NO
STATS
NOSTATS
(,INOPS)
(,NOINOPS)
(STATS,INOPS,NOINOPS)
(NOSTATS,INOPS,NOINOPS)
(16)
SECLVLCP
ADAPT
LEVEL1
LEVEL2
ADAPT
SIRFMSG
ALLSSCP
OLUSSCP
NONE
SLOWVAL
(0,0)
warn_time
(warn_time,end_time)
SLUALMSG
NOSUPP
SUPPRESS
NOSUPP
SMEAUTH
DISCARD
DISCARD
EXIT
KEEP
SNAMGMT
NO
YES
NO
SNAPREQ
1000
number_of_requests
(17)
SNVC
3
subnet_visit_count
SONLIM
(60,30)
(percent_1,percent_2)
(percent_1)
(,percent_2)
(18)
SORDER
APPN
ADJSSCP
APPN
APPNFRST
SUBAREA
SRCHRED
OFF
OFF
ON
(19)
SRCOUNT
10
number_of_search_requests
(20)
SRTIMER
30
number_of_seconds
(21)
SSCPDYN
YES
NO
YES
SSCPORD
PRIORITY
DEFINED
PRIORITY
SSDTMOUT
30
number_of_seconds
(22)
SSEARCH
YES
YES
NO
CACHE
APPNFRST
STRGR
ISTGENERIC
ISTGENERIC
NONE
structure_name
STRMNPS
ISTMNPS
ISTMNPS
NONE
structure_name
SUPP
NOSUP
NOSUP
INFO
WARN
NORM
SER



Notes:

1 The IQDCHPID option controls which IQD CHPID (and related subchannel devices) VTAM selects to dynamically build the iQDIO (IUTIQDIO) MPC group. The IUTIQDIO MPC group is used for TCP/IP dynamic XCF communications within System z. Although this option can be modified (and the modification will immediately be displayed) while the IUTIQDIO MPC group is currently active, any modifications have the effects shown in the section called IQD CHPID modifications.

2 This option affects only iQDIO devices that use a MFS of 64k. The smaller frame sizes will always use 126 SBALs. You can override this option on a per-device basis using the READSTORAGE parameter on the LINK or INTERFACE statement in the TCP/IP profile. See z/OS Communications Server: IP Configuration Reference for more details.

3 LIST can be entered by a VTAM operator only. If LIST is coded in an ATCSTR*xx* file, it is considered to be an error and is ignored.

4 Because of the volume of messages that can be generated, it is not recommended that this option be enabled during normal operation. Instead, it is recommended that this option be enabled (using the MODIFY VTAMOPTS command) on all necessary hosts only when trying to diagnose specific problems. After the problem has been diagnosed or documentation has been collected, this option should be disabled once again (using the MODIFY VTAMOPTS command).

5 LISTBKUP can be coded only in a start option file. If you enter it on the START command or at an operator prompt, VTAM will ignore it.

6 MAXLOCAT is meaningful only if NODETYPE is specified.

7 MULTPATH is meaningful only if the NODETYPE start option is also specified.

8 NNSPREF can be specified only if NODETYPE=EN is specified during VTAM START processing.

9 NODETYPE enables APPN function. The combination of HOSTSA, NODETYPE, and SACONNS determines the configuration (subarea node, interchange node, migration data host, network node, or end node).

10 NUMTREES is meaningful only if the NODETYPE=NN start option is also used.

11 PMTUD is meaningful only if the NODETYPE start option is also specified.

12 A VTAM operator cannot enter the PROMPT or NOPROMPT start option; it can be coded only in ATCSTR00. The value coded in ATCSTR00 is ignored if start options are entered on the START command or if VTAM finds an error in a start list. Upon finding an error in a start list, VTAM prompts the operator so that the operator can specify the option correctly.

13 QDIOSTG defaults to MAX for 64-bit (z/Architecture) machines and MIN for non 64-bit machines. You can override this option on a per-device basis using the READSTORAGE parameter on the LINK or INTERFACE statement in the TCP/IP profile. See z/OS Communications Server: IP Configuration Reference for more details.

14 RESUSAGE is meaningful only if the NODETYPE=NN start option is also used.

15 ROUTERES is meaningful only if the NODETYPE=NN start option is also used.

16 The SECLVLCP start option is meaningful only if the NODETYPE and VERIFYCP start options are also used.

17 SNVC is meaningful only if the BN=YES start option is also used.

18 SORDER is meaningful only in an interchange node or a migration data host.

19 SRCOUNT is meaningful only if the SRCHRED=ON start option is also used.

20 SRTIMER is meaningful only if the SRCHRED=ON start option is also used.

21 The SSCPDYN start option applies only for interconnected networks (that is, GWSSCP=YES is used).

22 SSEARCH is meaningful only if the NODETYPE=NN start option is also used.

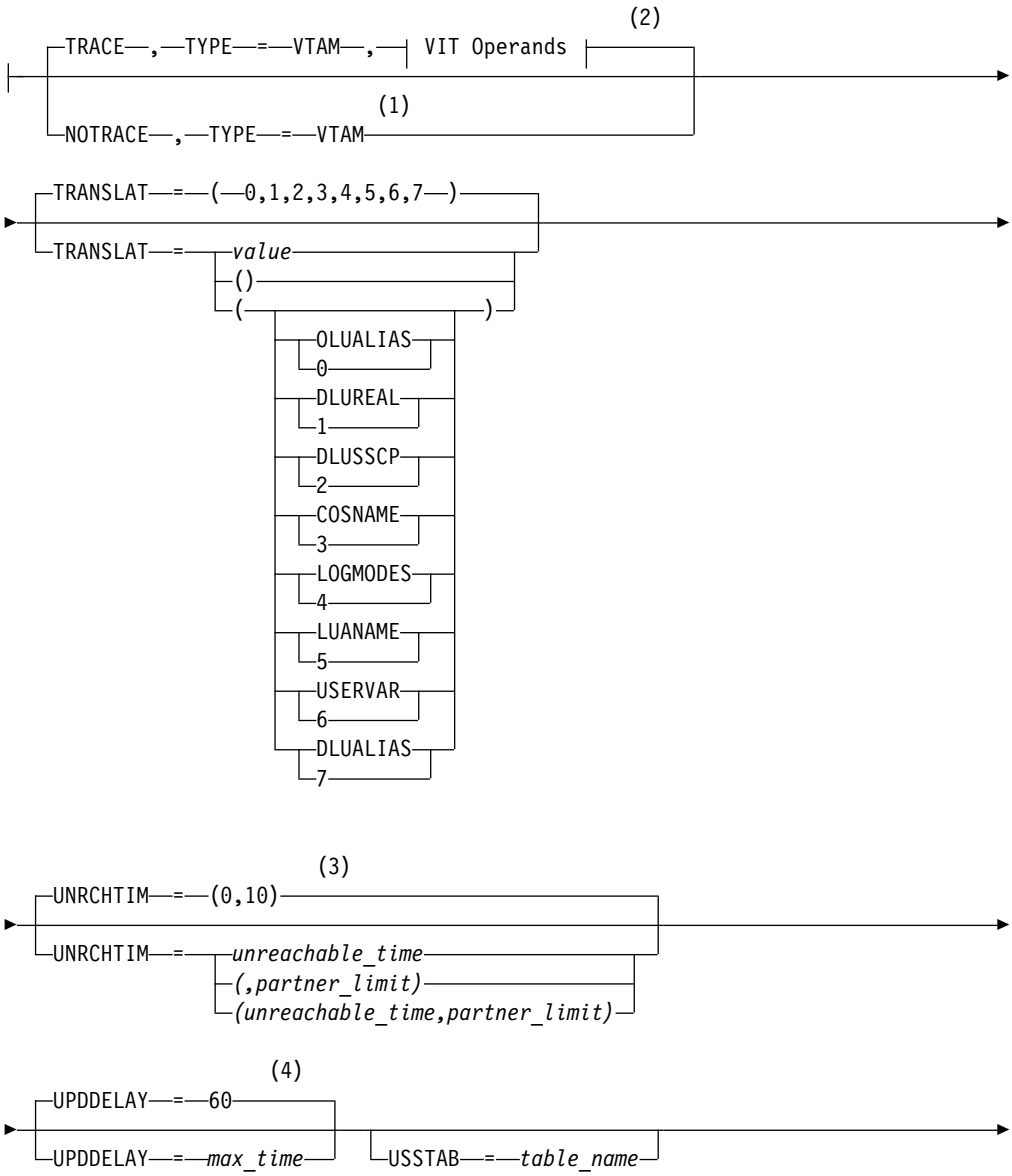
23 TCPNAME is meaningful only if the NODETYPE start option is also used. If neither IPADDR nor HOSTNAME is specified on any of the GROUP definition statements within the Enterprise Extender XCA major node, then either the HOSTNAME, TCPNAME, or IPADDR start options must be specified in order to activate an Enterprise Extender link.

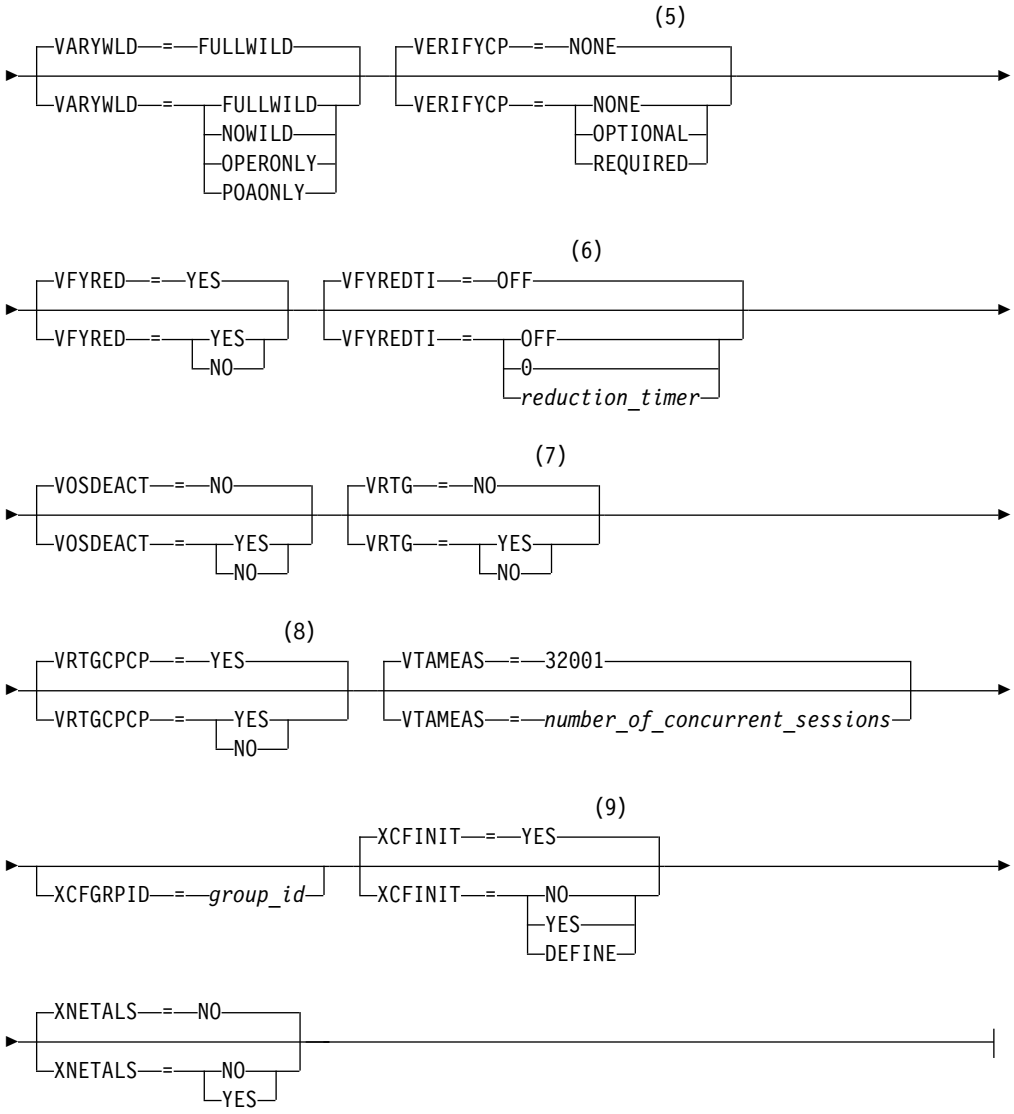
24 TDUDIAG is meaningful only if the NODETYPE=NN start option is also available.

25 TOPOTIME is meaningful only if the NODETYPE start option is also used.

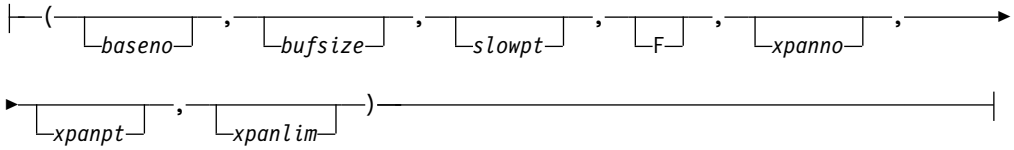
26 Do not use NOTRACE when starting VTAM, except to override a TRACE start option coded in a predefined list.

27 You can code TRACE and its qualifiers through position 71, even if you are in the middle of the start option. Continue the remainder of the item in the next record. Code the TYPE qualifier immediately after you code the TRACE start option.

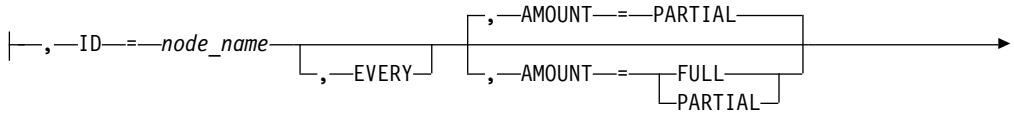


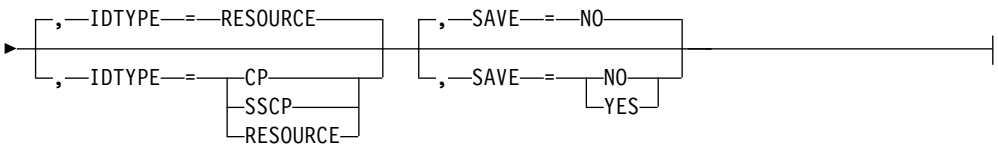


Buffer Pool Values:

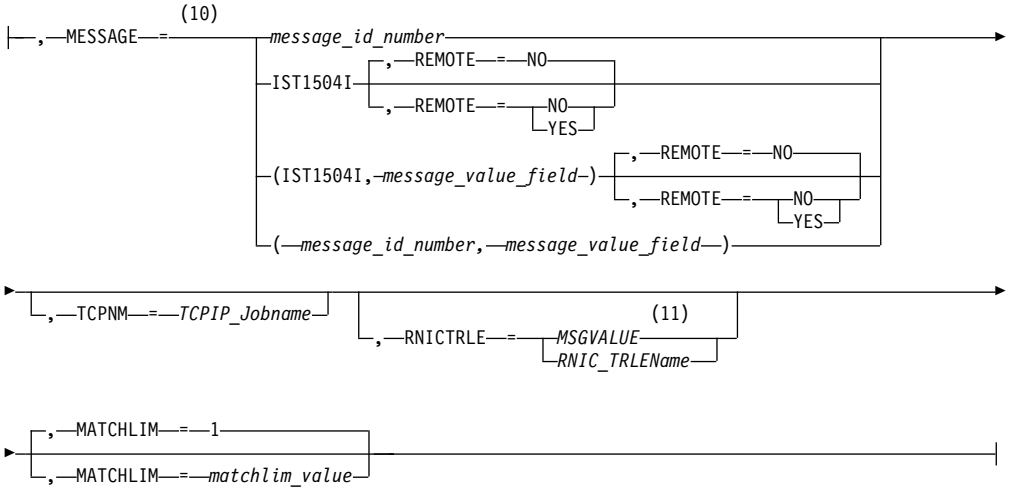


BUF Trace Operands:

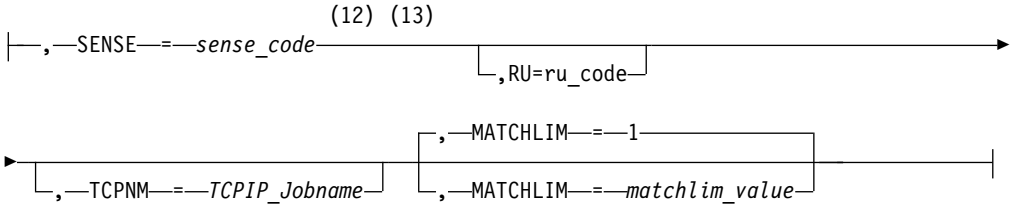




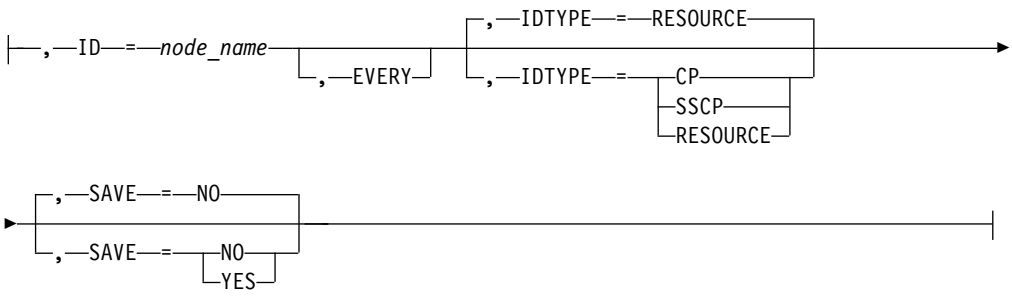
CSDUMP message trigger:



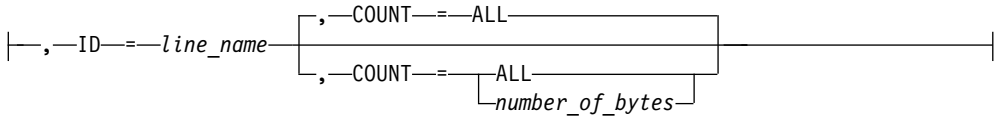
CSDUMP sense code trigger:



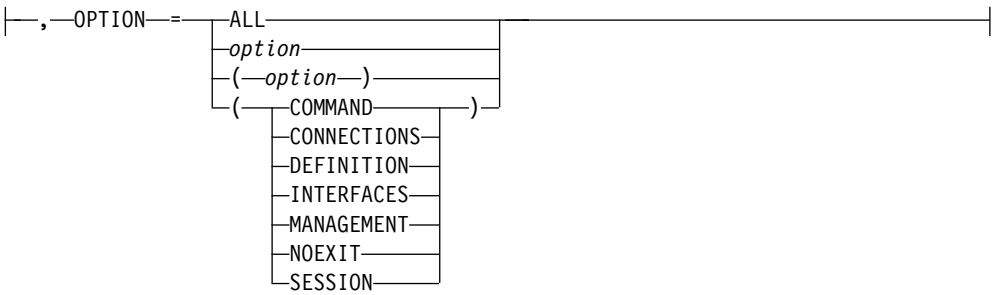
IO Trace Operands:



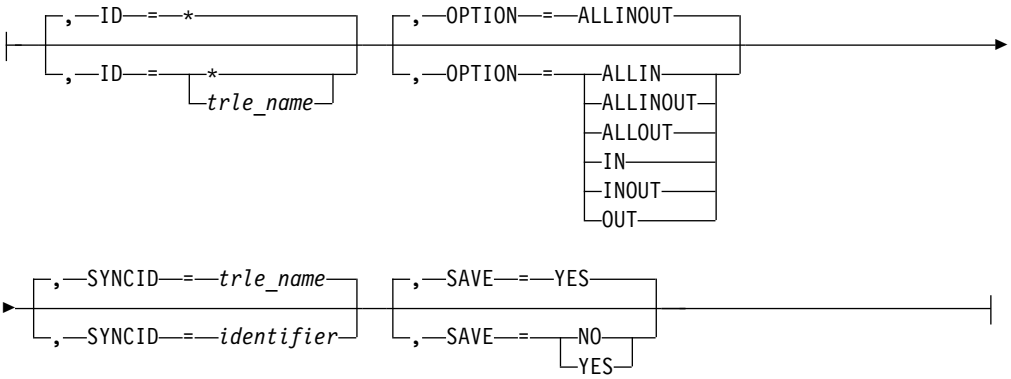
LINE Trace Operands:



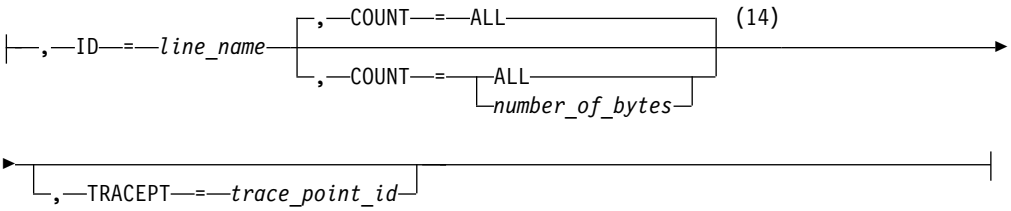
MODULE Trace Operands:



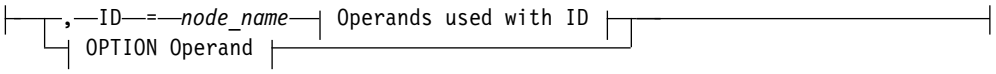
QDIOSYNC trace operands:



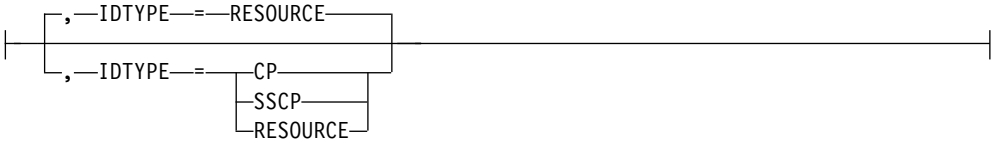
SIT Trace Operands:



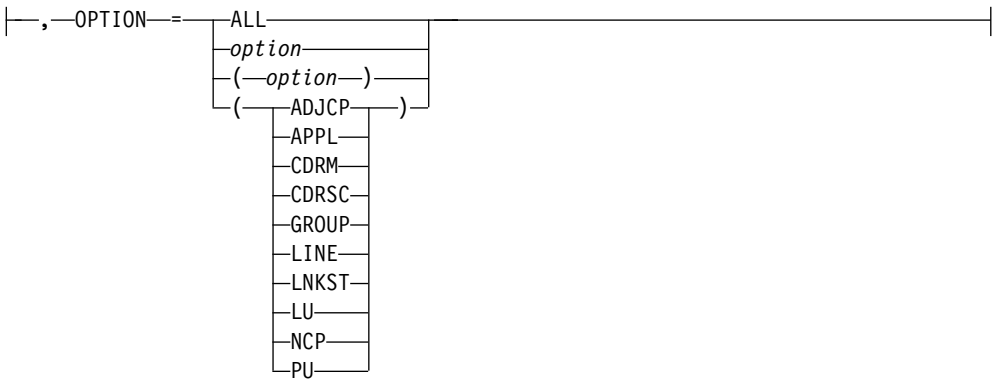
STATE Trace Operands:



Operands used with ID:



OPTION Operand:



Notes:

1 NOTRACE,TYPE=VTAM is accepted but ignored. Tracing is started with the default trace table size and the default options.

2 You can code TRACE and its qualifiers through position 71, even if you are in the middle of the start option. Continue the remainder of the item in the next record. Code the TYPE qualifier immediately after you code the TRACE start option.

3 UNRCHTIM is meaningful only if the NODETYPE start option is also used.

4 UPDDELAY is meaningful only if the OSIMGMT=YES start option is also used.

5 The VERIFYCP start option is meaningful only if the NODETYPE start option is also used.

6 VFYREDTI is meaningful only if the NODETYPE=NN start option is also used.

7 VRTG is meaningful only if the NODETYPE and HOSTSA start options are also used.

8 VRTGCPCP is meaningful only if the NODETYPE and HOSTSA start options are also used.

9 XCFINIT=YES is the default if VTAM is started as an APPN node (that is, the NODETYPE start option has been specified). XCFINIT=YES is not valid for pure subarea nodes. XCFINIT=DEFINE is the default if VTAM is started as a pure subarea node (the NODETYPE start option has not been specified).

10 When the same parameter is entered multiple times on a CSDUMP message trigger, only the last occurrence is accepted.

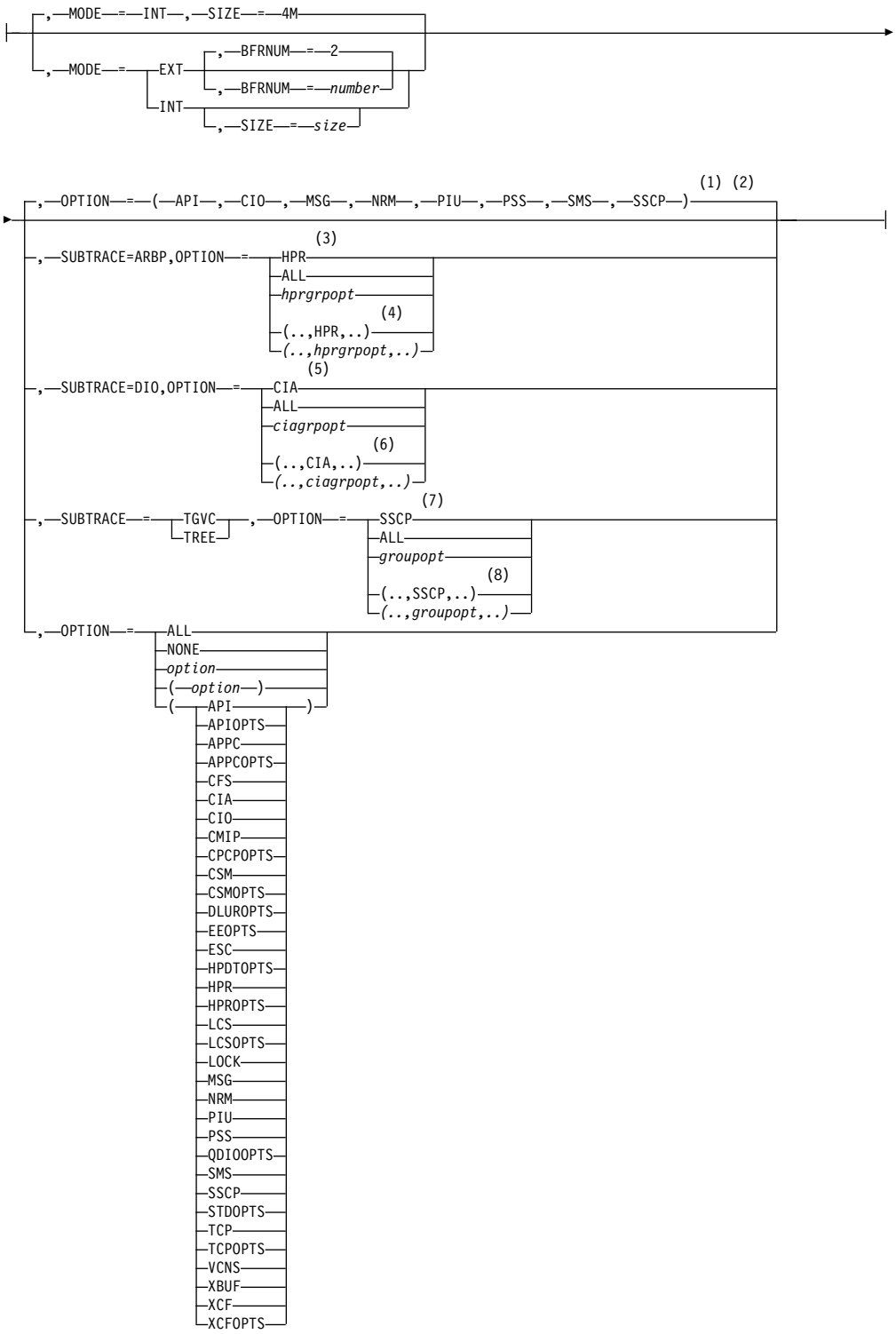
11 MSGVALUE is valid only when the MESSAGE operand is used and specifies either message IST2391I, IST2406I or IST2419I.

12 When an error message is received on any parameter of the CSDUMP start option, the remaining parameters for this CSDUMP start option are ignored. Enter the complete CSDUMP start option again when you are prompted.

13 When the same parameter is entered multiple times on a CSDUMP sense trigger, only the last occurrence is accepted.

14 COUNT applies only to the IBM 3720 and 3745 Communication Controllers.

VIT Operands:



Notes:

1 The default options apply only to MODE=INT.

2 PSS and SMS can be turned off.

3 When you specify SUBTRACE=ARBP and you code a single OPTION value,

the OPTION value must be HPR, ALL, or one of the group options (*hprgrpopt*) that include HPR as an individual option equivalent. The applicable group options are DLUROPTS, EEOPTS, HPDTOPTS, HPROPTS, QDIOOPTS, and XCFOPTS.

4 When SUBTRACE=ARBP is coded and you code multiple trace options in parentheses, you must code either HPR or one of the group options (*hprgrpopt*) that include HPR as an individual option equivalent inside the parentheses.

5 When you specify SUBTRACE=DIO and you code a single OPTION value, the OPTION value must be CIA, ALL, or one of the group options (*ciagrpopt*) that include CIA as an individual option equivalent. The applicable group options are EEOPTS, HPDTOPTS, HPROPTS, QDIOOPTS, TCPOPTS and XCFOPTS.

6 When SUBTRACE=DIO is coded and you code multiple trace options in parentheses, you must code either CIA or one of the group options (*ciagrpopt*) that include CIA as an individual option equivalent inside the parentheses.

7 When you code SUBTRACE=TGVC or SUBTRACE=TREE and you code a single OPTION value, the OPTION value must be either SSCP, ALL, or one of the group options (*groupopt*), all of which include SSCP as an individual option equivalent. The group options are APIOPTS, APPCOPTS, CPCPOPTS, CSMOPTS, DLUROPTS, EEOPTS, HPDTOPTS, HPROPTS, LCSOPTS, QDIOOPTS, STDOPTS, TCPOPTS, and XCFOPTS.

8 When you code SUBTRACE=TGVC or SUBTRACE=TREE and you code multiple trace options in parentheses, you must code either SSCP or one of the group options (*groupopt*) inside the parentheses.

IQD CHPID modifications

While the IUTIQDIO MPC group is currently active, any modifications to the IQDCHPID option have the following effects:

- Modified from ANY (or CHPID) to NONE - no effect on current usage but blocks subsequent activations
- Modified from NONE to ANY (or CHPID) - no effect on current usage but allows subsequent activations
- Modified from CHPID_X to CHPID_Y - no effect on current usage

Note: VTAM uses the CHPID value only when building the IUTIQDIO MPC group. To change CHPIDs for an active MPC group, the following must be done:

1. All TCP/IP iQDIO (HiperSocket) devices must be stopped.
2. Make any necessary HCD/IOCDS changes.
3. Verify that new subchannel devices are varied online.
4. Verify that the MPC group has deactivated (with no usage, it times out after approximately two minutes).
5. Modify IQDCHPID=CHPID (to new CHPID).
6. Restart the TCP/IP iQDIO device or devices.

Note: In order to use iQDIO communications, the processor must have the necessary hardware support. If the processor does not support iQDIO communications, then modifications to this start option will not be accepted and the IQDCHPID option will not be displayed (displayed as ***NA***).

Abbreviations

Operand	Abbreviation
START	S
AMOUNT=FULL	AMT=F
AMOUNT=PARTIAL	AMT=P
DATEFORM	DATEFRM
EVERY	E
MSGLEVEL	MSGLVL
OPTION	OPT
OPTION=COMMAND	OPT=CMD
OPTION=CONNECTION	OPT=CON
OPTION=DEFINITION	OPT=DEF
OPTION=INTERFACES	OPT=INT
OPTION=MANAGEMENT	OPT=MGMT
OPTION=SESSION	OPT=SES
PLUALMSG=NOSUPP	PLUALMSG=NOSUP
PLUALMSG=SUPPRESS	PLUALMSG=SUPP
SECLVLCP=LEVEL1	SECLVLCP=LVL1
SECLVLCP=LEVEL2	SECLVLCP=LVL2
SLUALMSG=NOSUPP	SLUALMSG=NOSUP
SLUALMSG=SUPPRESS	SLUALMSG=SUPP
TRANSLAT=COSNAME	TRANSLAT=3
TRANSLAT=DLUALIAS	TRANSLAT=7
TRANSLAT=DLUREAL	TRANSLAT=1
TRANSLAT=DLUSSCP	TRANSLAT=2
TRANSLAT=LOGMODES	TRANSLAT=4
TRANSLAT=LUANAME	TRANSLAT=5
TRANSLAT=OLUALIAS	TRANSLAT=0
TRANSLAT=USERVAR	TRANSLAT=6

When using an abbreviation in place of an operand, code the abbreviation exactly as shown in the table. For example, when coding the abbreviation for PLUALMSG=SUPPRESS, code only PLUALMSG=SUPP.

Purpose

VTAM is started with the START command.

You can enter the START command only at the master or a secondary system console.

Operands

procname
Procedure name for the command.

procname can be specified as either *startname.ident* or *startname*, where *startname* is the name of the JCL procedure used to start VTAM and *ident* is an optional identifier.

procname used for this command determines the *procname* used for all MODIFY commands as follows:

- If *procname* in the START command was specified as *startname.ident*, where *startname* is the VTAM start procedure and *ident* is the optional identifier, then either *startname.ident* or *ident* can be specified for *procname*.
- If *procname* in the START command was *startname*, then *startname* must be specified for *procname*.

Therefore, if you use NET as the optional identifier on this command, you can consistently use NET as *procname* for all VTAM commands.

options
VTAM start options supplied by the system programmer. The VTAM operator can enter one or more options. For a description of the start options, see z/OS Communications Server: SNA Resource Definition Reference.

If more than one line is necessary for the start options, enter a comma and a closing parenthesis after the last option.

The values established by the start options go into effect when VTAM is started and remain in effect until VTAM is halted. Many of the options, however, can be modified with the MODIFY VTAMOPTS command while VTAM is running. You can use the DISPLAY VTAMOPTS command to display the values of the start options.

Examples

```
s net,,,(list=01)s net,,,(list=01)
...
IST020I VTAM INITIALIZATION COMPLETE FOR level
IST1349I COMPONENT ID IS dddd-ddddd-ddd
IST1348I VTAM STARTED AS nodetype
```

For further information about these messages, see z/OS Communications Server: SNA Messages.

Chapter 9. SNA Network Implementation Guide

Resources automatically activated by VTAM

Certain resources are automatically activated by VTAM. Some internally maintained resources are automatically activated when the message "VTAM INITIALIZATION COMPLETE" is issued. These resources can be displayed, but cannot be activated or deactivated by an operator. The following resources are automatically activated:

- VTAMSEG application program major node:
  - VTAM (or name from the CDRM definition statement for this VTAM)
  - ISTATA00
  - ISTNOP
  - ISTPDCLU
  - ISTAPNCP
- VTAMSEG2 application program major node:
  - *?-?* (model application program definition for Telnet server shared ACBs)

  Note: The definition of the model application program for Telnet server shared ACB names cannot be displayed.
- ISTPUS PU (or name from HOSTPU start option) type 5 node
  - ISTGROUP
- ISTPDILU predefined independent LU major node
- ISTADJCP adjacent CP major node
- ISTCDRDY dynamic cross-domain resource major node

  Note: The ISTCDRDY major node can be deactivated and activated by an operator. For further information, see Dynamic definition of independent LUs.
- ISTRTPMN rapid transport protocol major node
- ISTTRL transport resource list major node
- ISTLSXCF local SNA major node

  Note: ISTLSXCF can also be deactivated and activated by the operator.

VTAM dynamically builds and activates transport resource list elements (TRLEs) within the ISTTRL major node for some TCP/IP communication interfaces. All of these TRLEs are created when needed, but cannot be deleted. These dynamic TRLEs are created with the following naming convention:

ISTT*lsrs*

TRLEs of this name are created when VTAM is started with either XCFINIT=YES (the default) or XCFINIT=DEFINE and another VTAM joins the XCF group (ISTXCF).

- *ls* is the two character &SYSCLONE value of the VTAM on the local MVS image
- *rs* is the two character &SYSCLONE value of the VTAM on the partner MVS image.

TCP/IP uses these TRLEs in one of the following situations:

- DYNAMICXCF is specified on the IPCONFIG or IPCONFIG6 statement and device or interface definitions are dynamically created to other VTAMs with XCF connectivity.
- DEVICE/LINK statements of type MPCPTP contain a device name that is the CPNAME or SSCPNAME of another VTAM with XCF connectivity.
- INTERFACE definitions of type MPCPTP6 contain a TRLENAME that is the CPNAME or SSCPNAME of another VTAM with XCF connectivity.

IUT0*pfid*
This TRLE is created when TCP/IP activates one of the following interfaces, which have the SMCD operand specified or taken as the default value, and Shared Memory Communications - Direct Memory Access (SMC-D) is enabled on the system:

- IPAQIDIO interface
- IPAQIDIO6 interface
- IPAQENET interface with CHPIDTYPE OSD
- IPAQENET6 interface with CHPIDTYPE OSD

The *pfid* value is discovered by VTAM during activation of the TRLE. No subchannels are associated with this TRLE.

IUTSAMEH
This TRLE is created for communication between multiple TCP/IP stacks on the same MVS image, and for communication between TCP/IP and VTAM for Enterprise Extender.

IUTIQDIO
This TRLE is created for TCP/IP dynamic XCF communications over HiperSockets devices. Up to 10 subchannel addresses are allocated: one READ and one WRITE device, and eight DATAPATH devices.

IUTIQD*xx*
This TRLE is created when TCP/IP activates a HiperSockets interface (defined by using either the DEVICE/LINK statements for IPAQIDIO or the IPv6 INTERFACE statement for IPAQIDIO6) with a CHPID parameter of *xx*. Up to 10 subchannel addresses are allocated: one READ and one WRITE device, and eight DATAPATH devices.

IUTIQ4*xx*
This TRLE is created when TCP/IP activates a HiperSockets interface (defined by using the IPv4 INTERFACE statement for IPAQIDIO) with a CHPID parameter of *xx*. Up to 10 subchannel addresses are allocated: one READ and one WRITE device, and eight DATAPATH devices.

IUTIQX*xx*
This TRLE is created for TCP/IP dynamic Internal Queued Direct I/O extensions (IQDX) function IPv4 communications over HiperSockets devices that are connected to the intraensemble data network (IEDN). The value *xx* is the OSX CHPID number that is associated with this IQDX TRLE. Up to 10 subchannel addresses are allocated: one READ and one WRITE device, and eight DATAPATH devices.

IUTIQ6*xx*
This TRLE is created for TCP/IP dynamic IQDX IPv6 communications over HiperSockets devices that are connected to the intraensemble data network (IEDN). The value *xx* is the OSX CHPID number that is associated with

this IQDX TRLE. Up to 10 subchannel addresses are allocated: one READ and one WRITE device, and eight DATAPATH devices.

IUTXT0*xx*
This TRLE is created when TCP/IP activates an MPCIPA INTERFACE with CHPIDTYPE OSX and a CHPID parameter of *xx*. Up to 19 subchannel addresses are allocated: one READ and one WRITE device, and 17 DATAPATH devices.

IUTMT0*xx*
This TRLE is created when TCP/IP activates a dynamically defined OSM interface, where VTAM assigned CHPID *xx* for this communication. Up to 11 subchannel addresses are allocated: one READ and one WRITE device, and nine DATAPATH devices.

IUT*npfid*
This TRLE is created when TCP/IP activates an IPAQENET or IPAQENET6 interface with CHPIDTYPE OSD with Shared Memory Communications - RDMA (SMC-R) specified or taken as the default, and SMC-R is enabled on the system. The *npfid* value is derived from the PORTNUM and PFID values on the SMCR parameter of the GLOBALCONFIG statement in the TCP/IP profile. For example, IUT20018 indicates that the PORTNUM value is 2 and the PFID value is 0018. If PORTNUM is not specified, the default value is 1. No subchannels are associated with this TRLE.

IUT*tdddd*
This TRLE is created when TCP/IP activates a CDLC, CLAW, Hyperchannel, CTC, or LCS device.

- *t* identifies the type of device that is dynamically created:
  - C - TCP/IP CDLC
  - W - TCP/IP CLAW
  - H - TCP/IP Hyperchannel
  - X - TCP/IP CTC
  - L - TCP/IP LCS
- *dddd* identifies the read device address for this device.

Gathering tuning statistics

By using the TNSTAT start option or the MODIFY TNSTAT command, you can collect data that will help you set the proper values on resource definition operands that control VTAM I/O operations in your system.

You can use VTAM tuning statistics to gather information about the following connections:

- SNA controller
- Channel-to-channel
- Multipath channel
- TCP
- Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE)

You cannot use VTAM tuning statistics to gather information about internal shared memory (ISM) devices. However, you can obtain some tuning statistics for ISM interfaces by using the Netstat DEvlinks/-d report. For more information, see Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands.

System management facility (SMF) is required to record tuning statistics. Tuning statistics can optionally be displayed at the system console using the CNSL operand, and statistics are always recorded in the appropriate tuning statistics file. This file is an SMF data set. The tuning statistics record is SMF record type 50. The format depends upon the resource for which the tuning I/O operation is collected. The tables in this section show the formats that can be present in a tuning statistics record.

TNSTAT need not be specified in the VTAM start list to later activate tuning statistics.

No tuning statistics are provided for LANs connected through XCA lines.

Tuning statistics can be activated or deactivated for all devices simultaneously (global tuning statistics), and tuning statistics can also be activated or deactivated based on a TRLE name (TRLE tuning statistics). When a TRLE is first activated, the tuning statistics state for that TRLE is set to the global tuning statistics state. For instance, if global tuning statistics are active, TRLE tuning statistics are active for that TRLE.

Chapter 10. SNA Diagnosis Volume 1: Techniques and Procedures

I/O trace

The I/O trace shows requests and responses that flow between VTAM and network nodes. You can trace I/O activity for any of the following types of nodes:

- Application program
- Physical unit
- Logical unit
- SNA cluster controller
- NCP
- SSCP
- Host physical unit
- Host as an intermediate routing node
- Channel attachment major node
- Cross-domain resource
- Cross-domain resource manager
- RTP pipe
- TRLE

  Restriction: I/O trace is not supported for a TRLE that represents an IBM 10GbE RoCE Express interface or an Internal Shared Memory (ISM) interface.

The maximum I/O trace record length is 272 bytes.

Note:

1. If you want to trace a session between an LU and an application program, you must start the trace at the host where the application program resides.
2. I/O trace records are not recorded for conversation level data exchanged between two VTAM/APPC applications residing on the same host and using the APPCCMD macroinstruction interface to communicate.
3. I/O trace provides packet tracing capability for OSA-Express QDIO and HiperSockets data devices because CCW trace does not exist for these devices. Packet trace for OSA-Express QDIO and HiperSockets will appear as ODPK records in the external VIT. A length field is provided on the MODIFY TRACE command for OSA-Express QDIO and HiperSockets devices to override the existing 272-byte trace limit for I/O trace.
4. Do not enable I/O trace for an OSA-Express2 or later data device that is used to capture OSA-Express network traffic analyzer trace data. The VARY TCPIP,,OSAENTA command described in z/OS Communications Server: IP Diagnosis Guide has its own ability to filter, capture, and format this data. If I/O trace is enabled for a data device used for capturing trace data, only the first 28 bytes of each packet are traced.
5. You must use a combination of the TCP/IP packet trace facility and VTAM internal trace (VIT) records to analyze Shared Memory Communications - RDMA (SMC-R) link traffic. The RPST records in the VIT represent data being sent outbound by using SMC-R communications. The RPLR records in the VIT

represent data arriving inbound by using SMC-R communications. For information about the TCP/IP packet trace, see z/OS Communications Server: IP Programmer's Guide and Reference.

6. You must use the TCP/IP packet trace facility to analyze Shared Memory Communications - Direct Memory Access (SMC-D) link traffic. For information about the TCP/IP packet trace, see z/OS Communications Server: IP Programmer's Guide and Reference.

Chapter 11. SNA Diagnosis Volume 2: FFST Dumps and the VIT

Trace options for the VIT

You can specify the OPTION operand in the TRACE start option or in the MODIFY TRACE command. Deactivate the VIT before you attempt to change an option; otherwise, the options that are currently in effect will remain in effect. See Deactivating the VIT for more information about deactivating the VIT.

Table 18 describes the options that you can specify on the OPTION operand. Select one or more of these options to indicate the VTAM functions you want to trace.

Table 18. Trace options of the OPTION operand

Option	Description
API option (for application programming interfaces)	This option helps you determine whether an application program is causing a problem. API entries are written for RPL macros, RPL exit routines, user exit routines, and user posts. Trace data for this option is always automatically recorded in the internal table.
APIOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose potential application program problems. Specifying the APIOPTS option is equivalent to specifying all the following VIT options: API, MSG, NRM, PIU, PSS, SMS, and SSCP.
APPC	This option helps you determine whether an LU 6.2 application is causing a problem. LU 6.2 entries are written for APPCCMD macro invocations, user posts, and exit scheduling by LU 6.2 code, calls to a security manager for security processing, and message unit transmissions between LU 6.2 components.
APPCOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose potential LU 6.2 application program problems. Specifying the APPCOPTS option is equivalent to specifying all the following VIT options: API, APPC, MSG, NRM, PIU, PSS, SMS, and SSCP.
CFS option (for coupling facility interfaces)	This option helps you determine problems with the VTAM interface with the MVS coupling facility. CFS entries are written when VTAM issues MVS macros to request services related to the coupling facility.
CIA option (for channel input and output auxiliary)	This option helps you isolate problems related to channel I/O CIA entries. This option presents the remaining trace records from the CIO option.
CIO option (for channel input and output)	This option helps you isolate problems related to channel I/O. CIO entries are written for attentions, error recovery, interruptions, HALT I/O SVC, and START I/O SVC.

Table 18. Trace options of the OPTION operand (continued)

Option	Description
CMIP option (for Common Management Information Protocol Services)	Setting the CMIP option enables the following traces: • Calls from CMIP application programs to the management information base (MIB) application programming interface (API) • Calls to the read-queue exit of the CMIP application program • Topology updates from VTAM resources You can use the CMIP option to help you determine whether there is a problem in VTAM or in a CMIP application program.
CPCPOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose potential CP-CP session problems. Specifying the CPCPOPTS option is equivalent to specifying all the following VIT options: API, APPC, MSG, NRM, PIU, PSS, SMS, and SSCP.
CSM option (for communications storage manager events)	This option traces the parameter list information that flows across the CSM interface and key internal events (such as pool expansion and contraction) for functions that manipulate buffer states. You can trace and analyze the usage history of a buffer. You can also use the CSM trace when VTAM is not operational. An external trace is generated using the VTAM GTF event ID to write trace records directly to GTF in the same format as those recorded using VIT.
CSMOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose potential communications storage manager (CSM) problems. Specifying the CSMOPTS option is equivalent to specifying all the following VIT options: API, APPC, CIO, CSM, MSG, NRM, PIU, PSS, SMS, SSCP, and XBUF.
DLUROPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose dependent LU requester (DLUR) problems. Specifying the DLUROPTS option is equivalent to specifying all the following VIT options: API, APPC, HPR, MSG, NRM, PIU, PSS, SMS, and SSCP.
EEOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose Enterprise Extender (EE) problems. Specifying the EEOPTS option is equivalent to specifying all the following VIT options: CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP, and TCP.
ESC option (for execution sequence control)	This option helps you track, in detail, the flow of requests for a given process.
HPDTOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose high-performance data transfer (HPDT) problems. Specifying the HPDTOPTS option is equivalent to specifying all the following VIT options: CIA, CIO, HPR, MSG, PIU, PSS, SMS, and SSCP.
HPR option (for High-Performance Routing)	This option helps you isolate problems related to High-Performance Routing.

Table 18. Trace options of the OPTION operand (continued)

Option	Description
HPROPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose High-Performance Routing (HPR) problems. Specifying the HPROPTS option is equivalent to specifying all the following VIT options: API, APPC, CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, and SSCP.
LCS option (for local area network (LAN) channel stations)	This option helps you isolate problems that occur when an IBM 3172 Interconnect Nways Controller is activating, deactivating, or transferring data. The LCS option enables tracing of data that VTAM receives from an IBM 3172 Interconnect Nways Controller at four levels: LCSX (channel), LCSP (port or adapter), LCSS (SAP), and LCSL (line).
LCSOPTS options	This option is a collection of multiple VIT options that includes all of the individual VIT options required to diagnose LAN channel station (LCS) problems. Specifying the LCSOPTS option is equivalent to specifying all the following VIT options: CIO, LCS, MSG, NRM, PIU, PSS, SMS, and SSCP.
LOCK option (for locking and unlocking)	This option helps you determine when VTAM modules obtain and release locks.
MSG option (for messages)	Specify this option to accomplish the following tasks: • Correlate other VIT entries with the console messages, even if you lose the console sheet. MSG entries are written for all messages to the VTAM operator. • Match the console log to a surge of activity shown in the VIT. OPER entries are written for all VTAM commands issued at an operator console. Trace data for this option is always automatically recorded in the internal table.
NRM option (for network resource management)	This option helps you follow the services of the network resource management component. These services include the assignment of, references to, and the deletion of certain VTAM resources such as node names, network addresses, and control blocks. NRM entries are written for SRT macros issued by VTAM modules. Trace data for this option is always automatically recorded in the internal table. CIDCTL FIND macro invocations used during the process of sending or receiving data are not traced with CDHF or CDNF trace entries unless they result in a nonzero return code.
PIU option (for path information unit flows)	This option, like the I/O and buffer contents traces, helps you isolate problems to hardware, to the NCP, or to VTAM. Unlike I/O and buffer contents traces, this option causes PIU entries to be written for all PIUs that flow internal and external to VTAM. Trace data for this option is always automatically recorded in the internal table.
PSS option (for process scheduling services)	This option helps you track the flow of requests through VTAM. PSS entries are written for the VTAM macros that invoke and control PSS, scheduling, and dispatching VTAM routines.

Table 18. Trace options of the OPTION operand (continued)

Option	Description
QDIOOPTS options	This option is a collection of multiple VIT options that includes all of the individual VIT options required to diagnose queued direct I/O (QDIO) problems. Specifying the QDIOOPTS option is equivalent to specifying all the following VIT options: CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, and SSCP.
SMS option (for storage management services)	This option helps you isolate problems caused by storage shortages. When you specify this option with the SSCP or PSS trace option, it can also help you isolate internal VTAM problems. SMS entries are written when SMS macros are used to request or free fixed-length or variable-length buffers. SMS entries are also written when VTAM expands or attempts to expand a buffer pool.
SSCP option (for system services control point request scheduling and response posting)	This option helps you isolate a VTAM problem to a specific VTAM component or module. SSCP entries are written for the request/response units (RUs) sent between VTAM components. This option also records information for the APPN CP. Trace data for this option is always automatically recorded in the internal table.
STDOPTS option	This option is a collection of multiple VIT options that includes all of the individual VIT options required to diagnose problems related to high CPU, session services, storage, Open/Close ACB, and DLCs such as multipath channel (MPC) and channel-to-channel (CTC). Specifying the STDOPTS option is equivalent to specifying all the following VIT options: API, CIO, MSG, NRM, PIU, PSS, SMS, and SSCP.
TCP option (for use with Enterprise Extender)	This option is used for recording activity related to Enterprise Extender. The trace options record IP address management and timer activity.
TCPOPTS option	This option is a collection of multiple VIT options that includes all of the individual VIT options required to diagnose problems related to TCP/IP. Specifying the TCPOPTS option is equivalent to specifying all the following VIT options: CIA, CIO, MSG, NRM, PIU, PSS, SMS, SSCP, and TCP.
VCNS option (for VCNS application programming interfaces)	This option helps you determine whether a VCNS application is causing a problem. VCNS entries are written for VCNSCMD macro invocations, user posts, exit scheduling by VCNS code, and work element transmissions between VCNS components.
XBUF option (for applications that use the extended buffer list for sending and receiving data)	This option traces the contents of the extended buffer list (XBUFLST). Records are produced to trace these contents from the application-supplied extended buffer list and the internal buffer list that VTAM uses to carry the extended buffer list information. These records store relevant information contained with the extended buffer list, particularly information about CSM usage by VTAM.
XCF option (for VTAM use of the cross-system coupling facility)	Specify this option to track VTAM use of the XCF (cross-system coupling facility) MVS macro interface. Each VTAM use of an XCF macro has a VIT entry.
XCFOPTS option	This option is a collection of multiple VIT options that includes all of the individual VIT options required to diagnose cross-system coupling facility (XCF) problems. Specifying the XCFOPTS option is equivalent to specifying all the following VIT options: CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP, and XCF.

The VIT always traces the exception conditions listed in Table 19 and all the default VIT options listed under Activating the VIT.

Table 19. Exception conditions always traced by the VIT

Option	Exception conditions traced
APPC	• ACA and ACI entries when following commands are issued: – SEND ERROR – DEALLOC ABNDxxxx – REJECT • ACRC and ACSN entries • Other entries with nonzero return codes (except RPL6RCSC)
CFS	Entries with nonzero return codes
CIO	INOP entry
CMIP option	The following entries, when they have nonzero return codes: • MCO1 and MCO2 • MDEL • MDIS • MQRQ • MQRS • MREG • RQE
LCS	LCSL, LCSP, LCSS, and LCSX entries with nonzero reason codes
NRM	CDHF or CDNF entries with nonzero return codes
SMS	Entries with nonzero return codes and EXPN entries if a buffer pool expansion fails
SSCP	CPI, CPO, and CP2
(No option)	All SNAP entries and some exception entries[1].

Note:

1. The **** (FFST™ and PFFST), ABND, BUFF, COPY, CMER, CME2, INOP, LOST, MMG, and MM2 trace records are not activated by specific VIT options. They are activated as a result of exception conditions.

Table 20 on page 608 and Table 21 on page 609 list the VIT options and the records that they create. For more information, see the list of notes after Table 21 on page 609.

Table 20. VIT options and the records they create (API - LOCK)

VIT options	API	APPC	CFS	CIA	CIO	CMIP	CSM	ESC	HPR	LCS	LOCK
VIT records								ESC		LCSx	
	AIx	ACAx	CFAx	CCR	ADE	MCO1	ASNx		ARB		LKEX
	IOx	ACIx	CFCx	CDSQ	ATT	MCO2	CHGx		ARBB		LKSH
	RE	ACPx	CFDx	C64Q	ERPx	MDEL	CNTP		ARBR		ULKA
	UEx	ACRx	CFEx	DEVx	HIOx	MDIS	CPYx		ARPx		UNLK
	UP	ACSN	CFFC	DRBx	INTx	MQRQ	EXPP		ARQx		
		ACUx	CFLx	ENFx	PCIT	MQRS	FIXx		ARSx		
		MUx	CFNF	GCEL	PCIX	MREG	FRBx		DAPT		
		RACR	CFPx	GCEx	RDVX	MRGx	GTBx		DRPx		
		REML	CFRB	HCRx	RIOx	RQE	PAGx		HCLK		
		REMQ	CFTx	ICRx	SIOx				HPRx		
		USx	CFUS	IDx					HPRT		
		UVx	CFVC	IOSx					NLPx		
			MNPS	IPLx					ONLP		
				ISPx					OOSx		
				IUTx					RCM		
				LNKx					RCV		
				LSNx					REML		
				MPDx					RSCx		
				ODPx					RTP		
				ODTx					RTPx		
				PCIx					RTSx		
				PKx					RVM		
				PLOQ					RXMT		
				P64Q							
				QAPL							
				QDIP							
				QSRx							
				RCPI							
				RCPO							
				RPLx							
				RPST							
				RSLK							
				SBAx							
				SIGA							
				SLSx							
				TOKx							
				VHCR							
				XIDx							

Table 21. VIT options and the records they create (MSG - XCF)

VIT options	MSG	NRM	PIU	PSS	SMS	SSCP	TCP	VCNS	XBUF	XCF
VIT records	MSGx OPEx QRYL TRNx	BSPx BSSx BSXx CDHx CDNx NIPx PROx RCEx SRTx	DCOx DSCx NRSx PIUx RDSx TSNS	ATSK BTSK DSP DTSK ETSK EXIT IRBx POST QUEx RESM SCHD SRBx VPST VRSM VWAI WAIT XPST	AREL CONT EXPN FBLx FRES GBLx GETS ORMG POOF QREx RAPx RELS REQx VTAL VTFR	AFSM ALSx AP A2 CCx CIx COx CPI CPO CP2 CPPx CPRx CPWx CRx CSx DBx DLTx ENR GNAx HLSx LDLx MT SPTx TGMx TGVx TOPx TPN2 TPTx TREx TRMx TRRx	IPAD IPGN IPG2 IPG3 IPOG IPO2 IPTC IPTM	CNA CNPx CNRx NSD VCCx VCDQ	XBAx XBIx XB6x	XCC2 XCFC XCFJ XCFL XCFM XCFR XCFS XCFX XCJ2 XCL2 XCM2 XCR2 XCS2

Note:

1. The **** (FFST and PFFST), ABND, BUFF, COPY, CMER, CME2, INOP, LOST, MMG, and MM2 trace records are not activated by specific VIT options. They are activated as a result of exception conditions.
2.
   - For CIO record types ATT, ERP, HIO, INT, SIO, with suffix I, X, or T, and INOP, the events are also captured in the NCB (pointed to by NCBCIOMV). The NCB trace table is mapped by NCBCIOAR.
   - For CIA record types INOP, RCPx, RPLx and RPST, the events are also captured in the RUNCB (pointed to by NCBCIOMV).
   - For CIA record type PCIR, the events are also captured in the SRNCB (pointed to by NCBCIOMV).
3. OON and OOX can be generated when the module trace is running.
4. For the IRBx and the SRBx records to be recorded, both the PSS trace option and the PSSTRACE start options must be specified.
5. For APPC record types REMQ and ACSN, the events are also captured in the ISTRAB.
6. Some trace records are generated only when a subtrace is active. These trace records are the HPR option record types ARBB, ARBR, the CIA option record types QAPL, QDIP, QSRx, RSLK, and the SSCP option record types HLSx,

TGVx, TRMx, and TRRx. For more information about subtraces, see z/OS Communications Server: SNA Operation.

Table 22 lists the VIT group options and the individual VIT options that are equivalent for each group option.

Table 22. VIT group options

VIT group option	Equivalent to this set of individual VIT options
APIOPTS	API, MSG, NRM, PIU, PSS, SMS, SSCP
APPCOPTS	API, APPC, MSG, NRM, PIU, PSS, SMS, SSCP
CPCPOPTS	API, APPC, MSG, NRM, PIU, PSS, SMS, SSCP
CSMOPTS	API, APPC, CIO, CSM, MSG, NRM, PIU, PSS, SMS, SSCP, XBUF
DLUROPTS	API, APPC, HPR, MSG, NRM, PIU, PSS, SMS, SSCP
EEOPTS	CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP, TCP
HPDTOPTS	CIA, CIO, HPR, MSG, PIU, PSS, SMS, SSCP
HPROPTS	API, APPC, CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP
LCSOPTS	CIO, LCS, MSG, NRM, PIU, PSS, SMS, SSCP
QDIOOPTS	CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP
STDOPTS	API, CIO, MSG, NRM, PIU, PSS, SMS, SSCP
TCPOPTS	CIA, CIO, MSG, NRM, PIU, PSS, SMS, SSCP, TCP
XCFOPTS	CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP, XCF

AFSM entry for altering an FSM state

Entry: AFSM

VIT option:
SSCP

Event: Alteration of an FSM state

VIT processing module:
ISTRACSC

Control is returned to:
The module that issued the INTRACE macroinstruction

This trace record is written when the current state of an FSM changes.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
AFSM				ASID	0	DLC TYPE	FSM TYPE	OLD STATE	NEW STATE	WKE TYPE	INSTANCE	RESOURCE ADDRESS				RETURN ADDRESS				WORK ELEMENT ADDRESS				MODULE NAME				RPH ADDRESS			

Byte (hex)
Contents

00–03 Record ID: C"AFSM"

04 ID is the primary address space ID (ASID). This field is 0 if the ASID is greater than X'FF'.

05 0

06 Data link control type:

- **A** ATM
- **E** Enterprise Extender
- **L** LAN (External Communication Adapter)
- **S** Shared Memory Communications

07 FSM type:

- **A** AAL FSM (ATM only)
- **D** LDLC FSM
- **E** LDLC XID FSM
- **I** Shared Memory Communications - Direct Memory Access (SMC-D) FSM
- **L** Link FSM
- **P** Port FSM
- **R** RDMA over Converged Ethernet (RoCE) user FSM
- **S** Shared Memory Communications over Remote Direct Memory Access (SMC-R) FSM
- **X** XID FSM

08 Old state

09 New state

0A Work element type:

- **01** ISTRPH
- **17** ISTAUCPL
- **40** ISTLSPL
- **54** ISTRUPE
- **58** ISTTQE
- **99** IUTTIPAC
- **9A** ISTTSPL
- **9B** ISTLSCB

0B 0 or instance of the SETAFSM macro in the module

0C–0F Address of the control block containing the FSM

10–13 Return address of the module that changed the FSM state

14–17 Work element address

18–1B Name of the module that changed the FSM state

1C–1F Request parameter header (RPH) address

ICR entry for a control register operation

Entry: ICR

VIT option:
CIA

Event: Internal shared memory (ISM) control register operation

This trace record is written when an ISM control register operation is performed to manage an ISM interface as part of Shared Memory Communications - Direct Memory Access (SMC-D) processing.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
ICR				ASID	0	MODULE		ID		RETURN		CODE		REASON		CODE		COMMAND		RESULT		CODE		SLNCB ADDRESS				HARDWARE		HANDLE		RPH ADDRESS	

Byte (hex)
Contents

00–03 Record ID: C'ICR'

04 ID is the primary address space ID (ASID). This field is 0 if the ASID is greater than X'FF'.

05 0

06–07 Two-character identifier of the module that issued the control register operation

08–09 Return code

0A–0B Reason code

0C–0F Command result code

10–18 Address of the SLNCB control block that represents the ISM interface

19–1B Hardware handle

1C–1F Request parameter header (RPH) address

ICR2 entry for a control register operation (part 2)

Entry: ICR2

VIT option:
CIA

Event: Internal shared memory (ISM) control register operation

This trace record is a continuation of the ICR record, and is generated only when the ISM control register operation requires command input data. Multiple ICR2

entries might be generated, depending on the length of the command input data.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
I C R 2	28 BYTES OF COMMAND INPUT DATA																														

Byte (hex)
Contents

00–03 Record ID: C'ICR2'

04–1F Command input data

ICR3 entry for a control register operation (part 3)

Entry: ICR3

VIT option:
CIA

Event: Internal shared memory (ISM) control register operation

This trace record is a continuation of the ICR record, and is generated only when the ISM control register operation produces command output data. Multiple ICR3 entries might be generated, depending on the length of the command output data.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
I C R 3	28 BYTES OF COMMAND OUTPUT DATA																														

Byte (hex)
Contents

00–03 Record ID: C'ICR3'

04–1F Command output data

IOSP entry for invoking a Peripheral Component Interconnect Express (PCIe) service (Part 1)

Entry: IOSP

VIT option:
CIA

Event: Invocation of a Peripheral Component Interconnect Express (PCIe) service, as part of Shared Memory Communications over Remote Direct Memory Access (SMC-R) processing, or as part of Shared Memory Communications - Direct Memory Access (SMC-D) processing.

VIT processing module:
ISTITCSH

This trace record is written upon completion of a PCIe service.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
I	O	S	P	ASID	COMMAND	MODULE ID		ASSOCIATED PARMLIST ADDR								PFCTE ADDRESS -or- SLNCB ADDRESS								RETURN CODE		REASON CODE		RPH ADDRESS			

Byte (hex)
Contents

00–03 Record ID: C"IOSP"

04 ID is the primary address space ID (ASID). This field is 0 if the ASID is greater than X'FF'.

05 PCIe service identifier:

- 'A' for allocate service (IQP4ALL)
- 'C' for connect service (IQP4CON)
- 'D' for deallocate service (IQP4DEA)
- 'G' for get attribute service (IQP4GDI)
- 'L' for close service (IQP4CLO)
- 'M' for deregistration service (IQP4DMR)
- 'O' for open service (IQP4OPN)
- 'P' for get PFID attribute service (IQP4GPI)
- 'Q' for query system characteristics (IQP4QSC)
- 'R' for registration service (IQP4RMR)
- 'S' for search service (IQP4SRC)

06–07 Module identifier of the module that issued the INTRACE command

08–0F Input parameter list that is associated with the PCIe service

10–17 Address of the PFCTE or SLNCB

18–19 Return code

1A–1B Reason code

1C–1F Request parameter header (RPH) address

IOS2 entry for invoking a Peripheral Component Interconnect Express (PCIe) service (Part 2)

Entry: IOS2

VIT option:
CIA

Event: Invocation of a Peripheral Component Interconnect Express (PCIe) service, as part of Shared Memory Communications over Remote Direct Memory

Access (SMC-R) processing, or as part of Shared Memory Communications - Direct Memory Access (SMC-D) processing.

VIT processing module:
ISTITCSH

This trace record is a continuation of the IOSP record.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
I O S 2				PFID				CONN TOKEN								OPERATION HANDLE															

Byte (hex)
Contents

00-03 Record ID: C'IOS2'

04-07 The Peripheral Component Interconnect Express (PCIe) function ID (PFID)

08-0F Connection token that is associated with the PCIe service

10-1F Operation handle that is associated with the PCIe service

IOS3 entry for invoking a Peripheral Component Interconnect Express (PCIe) service (Part 3)

Entry: IOS3

VIT option:
CIA

Event: Invocation of a Peripheral Component Interconnect Express (PCIe) service, as part of Shared Memory Communications over Remote Direct Memory Access (SMC-R) processing, or as part of Shared Memory Communications - Direct Memory Access (SMC-D) processing.

VIT processing module:
ISTITCSH

This trace record is a continuation of the IOSP trace record when the record represents a register (IQP4RMR) command.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
I O S 3				KEY	0			MEMORY REGION ADDRESS								MEMORY REGION LENGTH								DMA ADDRESS OR ZEROES							

Byte (hex)
Contents

00–03 Record ID: C'IOS3'

04 Storage key

05–07 0

08–0F Address of the memory region

10–17 Length of the memory region

18–1F DMA address to be registered, or 0

IPLE entry for an internal shared memory (ISM) polling operation

Entry: IPLE

VIT option:
CIA

Event: Invocation of internal shared memory (ISM) event queue polling

This trace record is written when VTAM polls the ISM interface event queue and passes the information to the owning TCP/IP stack as part of Shared Memory Communications - Direct Memory Access (SMC-D) processing.

00 01 02 03	04	05 06	07	08 09	0A 0B	0C 0D 0E 0F	10 11 12 13 14 15 16 17	18 19 1A 1B	1C 1D 1E 1F
IPLE	ID	LWI	COUNT	RETURN CODE	REASON CODE	SLNCB ADDRESS	PARAMETER LIST ADDRESS	CALLER RETURN ADDRESS	RPH ADDRESS

Byte (hex)
Contents

00–03 Record ID: C'IPLE'

04 ID is the primary address space ID (ASID). This field is 0 if the ASID is greater than X'FF'.

05–06 Last written index on the ISM event queue

07 Number of events reported to the TCP/IP stack

08–09 Return code

0A–0B Reason code

0C–0F Address of the SLNCB control block that represents the ISM interface

10–18 Address of the parameter list (PList) provided to the TCP/IP stack

19–1B Return address of the module issuing the poll request

1C–1F Request parameter header (RPH) address

IPLA entry for an internal shared memory (ISM) polling operation (part 2)

Entry: IPLA

VIT option:
CIA

Event: Invocation of internal shared memory (ISM) event queue polling

This trace record is a continuation of the IPLE record. Multiple IPLA entries can be generated, one for each array entry that contains data at the completion of the PollEQ operation. A single Poll operation can have up to 64 array entries with data.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
I	P	L	A	EVENT TYPE				EVENT CODE				0		EQE NUMBER		EVENT TOKEN								EVENT DEBUG							

Byte (hex)
Contents

00–03 Record ID: C'IPLA'

04–07 Event Type:

- **0** DMB Event
- **1** GID Event
- **2** Software Requested Event

08–0B Event code:

- **1** GID in error state
- **2** Owning function in error state
- **3** Using function in error state
- **4** DMB was unregistered
- **5** VLAN mismatch with owner
- **6** VLAN mismatch with user
- **7** GID disabled
- **8** Using function disabled

0C–0D
0

0E–0F Event Queue Element (EQE) number

10–17 Event Token

18–1F Event Debug Information

ISPx entry for invoking an internal shared memory (ISM) Verb (part 1)

Entry: **ISPx**

VIT option:
CIA

Event: Invocation of an internal shared memory (ISM) verb as part of Shared Memory Communications - Direct Memory Access (SMC-D) processing.

VIT processing module:
ISTITCSH

Control is returned to:
The module that issued the INTRACE macroinstruction

This trace record is written when an ISM verb is invoked or when an ISM verb invocation is completed.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
I I	S S	P P	I O	I D	I N S T A N C E	P A R M L I S T	L E N G T H	RELATED CONTROL BLOCK				0				SLNCB ADDRESS				PLIST ADDRESS				M O D U L E	I D E N T I F I E R	P F I D		RPH ADDRESS			

Byte (hex)
Contents

00–03 Record ID:
- C'ISPI' for ISM parameter list information prior to the ISM verb invocation
- C'ISPO' for ISM parameter list information after the ISM verb invocation

04 ID is the primary address space ID (ASID). This field is 0 if the ASID is greater than X'FF'.

05 Instance identifier within the module

06–07 Length of the parameter list (PList) that is used for the ISM verb invocation

08–0B A related control block for this particular ISM verb

0C–0F 0

10–13 Address of the SLNCB control block that represents the ISM interface

14–17 Parameter list address. This is a 64-bit address, but only the lower 32 bits are shown in the trace record.

18–19 Last two characters of the module that issued the ISM verb

1A–1B Peripheral Component Interconnect Express (PCIe) function ID (PFID) that defines the ISM device that was the target of the ISM verb, in hexadecimal.

1C–1F Request parameter header (RPH) address

ISP2 entry for invoking an internal shared memory (ISM) Verb (part 2)

Entry: ISP2

VIT option:
CIA

Event: Invocation of an internal shared memory (ISM) verb as part of Shared Memory Communications - Direct Memory Access (SMC-D) processing when the input area in the ISM verb parameter list (PList) has non-zero information.

VIT processing module:
ISTITCSH

This trace record is continuation of the ISPI and ISPO entry. Multiple ISP2 entries may be generated, depending on the length of the input area in the PList that is used for the ISM verb.

00 01 02 03	04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
I S P 2	28 BYTES OF PLIST INPUT AREA

Byte (hex)
Contents

00–03 Record ID: C'ISP2'

04–1F 28 bytes of the input area in the PList

ISP3 entry for invoking an internal shared memory (ISM) Verb (part 3)

Entry: ISP3

VIT option:
CIA

Event: Invocation of an internal shared memory (ISM) verb as part of Shared Memory Communications - Direct Memory Access (SMC-D) processing when the output area in the ISM verb parameter list (PList) has non-zero information.

VIT processing module:
ISTITCSH

This trace record is continuation of the ISPO entry. Multiple ISP3 entries may be generated, depending on the length of the output area in the PList used for the ISM verb.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
I	S	P	3	28 BYTES OF PLIST OUTPUT AREA																											

Byte (hex)
Contents

00–03 Record ID: C'ISP3'

04–1F 28 bytes of the output area in the PList

IUTX mapping and field descriptions

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
IUTX				ID	DLC TYPE	FUNCTION		DQA ADDRESS or 0 or SMRQA ADDRESS				NCB ADDRESS				RETURN ADDRESS				ELEMENT COUNT				CALLED EXIT ADDRESS				THREAD ADDRESS or RPH ADDRESS			

Byte (hex)
Contents

00–03 Record ID: C"IUTX" for exit call

04 ID is the primary address space ID (ASID). This field is 0 if the ASID is greater than X'FF'.

05 DLC type:
- C'Q' for QDIO
- C'S' for Shared Memory Communications over Remote Direct Memory Access (SMC-R) and Shared Memory Communications - Direct Memory Access (SMC-D)

06–07 Function:
- C'WC' for write completion exit
- C'RC' for read completion exit
- C'SC' for SMC-D data completion exit
- C'EC' for SMC-D event completion exit

08–0B Queue Data address that is associated with the event
- If DLC type is 'Q', this field is a DQA address
- If DLC type is 'S' and Function is 'WC', this field is a SMRQA address
- If DLC type is 'S' and Function is 'SC' or 'EC', this field is a SMLQA address

- Otherwise, this field is 0.

0C–0F NCB address that is associated with IUTIL processing:
- If DLC type is 'Q', this is a DINCB address.
- If DLC type is 'S' and Function is 'WC' or 'RC', this is an RUNCB address.
- Otherwise, this is an SLNCB address.

10–13 INTRACE invoker

14–17 Number of elements on queue

18–1B Exit address

1C–1F Thread address or request parameter header (RPH) address:
- If DLC type is 'Q', the thread value or 0
- If DLC type is 'S', the RPH address

IUT6 mapping and field descriptions

IUT6 mapping and its detailed field descriptions, including different byte and contents are defined in this topic.

00 01 02 03	04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
IUT6	0	CONTAINER ADDRESS or SBA ADDRESS	0

Byte (hex)
Contents

00 - 03 Record ID: C"IUT6"

04 - 07 0

08 - 0F
Container address or SBA address
- If this record is immediately preceded by an IUTD record, this is a SPAC address.
- If this record is immediately preceded by an IUTX record where DLC Type is 'S' and Function is 'WC' or 'RC', this is a PLAC address.
- If this record is immediately preceded by an IUTX record where DLC Type is 'S' and Function is 'SC' or 'EC', this is an SBA address.

10 - 1F
0

PCIx entry for program-controlled or suspend interrupt

Entry: PCID, PCII, PCIR, PCIT, or PCIX

VIT option:
PCID, PCII, and PCIR: CIA

PCIT and PCIX: CIO

Event: Program-controlled or suspend interrupt

VIT processing module:
ISTITCOD

Control is returned to:
ISTTSCIE, ISTLLCIE, ISTSRRIE, ISTSICIE

This trace record is written when a program-controlled interrupt occurs.

This interrupt occurs for a CLAW channel-to-channel attached host, for HPDT read and write devices, or for the OSA-Express QDIO, Shared Memory Communications over Remote Direct Memory Access (SMC-R), Shared Memory Communications - Direct Memory Access (SMC-D), or the HiperSockets adapter read queue.

The PCID entry is recorded when the OSA-Express QDIO or HiperSockets adapter has completed a read operation. The PCID entry may or may not be preceded by a SIGA (read) operation for the same device.

The PCIT and PCIX entries are correlated to the SIOx, RIOx, and INTx entries for the same device using the CUA field. The combination of the information provided by these entries describe the channel program management and I/O operations for the device.

The PCIR entry is recorded when the IBM 10Gbe RoCE Express feature completes a read operation or encounters an error condition. The PCIR entry is followed by the RPLE, RPLP, and RPLA (optional) entries. These entries include information that describes the type and destination of the data received or the type of the error encountered.

The PCII entry is recorded when the internal shared memory (ISM) device completes a write operation or encounters an error condition.

See for a description of the NCB fields.

The PCIT and PCIX entries are also captured within the NCB (pointed to by NCBCIOMV). The NCB trace table is mapped by NCBCIOAR.

PCIR and PCII mapping and field descriptions

00 01 02 03	04 05 06 07	08 09 0A 0B	0C 0D 0E 0F	10 11 12 13 14 15 16 17	18 19 1A 1B 1C 1D 1E 1F
PCIR PCII	ID 0 REASON	PFID VALUE	FLAGS 0 RETCODE	PFCTE ADDRESS or SLNCB ADDRESS	TIME STAMP OF PCI EVENT

Byte (hex)
Contents

00–03 Record ID:

- C'PCII' for SLNCB
- C'PCIR' for SRNCB

04 ID is the primary address space ID (ASID). This field is 0 if the ASID is greater than X'FF'.

05-06 0

07 Interrupt reason

- C'C' when the interrupt is driven as a result of a completed work request
- C'D' when the interrupt is driven as a result of device deallocation
- C'E' when the interrupt is driven as a result of a device error
- C'V' when the interrupt is driven as a result of the adapter interrupt monitoring function

08–0B Peripheral Component Interconnect Express (PCIe) function ID (PFID) that is associated with the interrupt

0C

- Summary flags for PCII event
- 0 for PCIR event

0D–0E 0

0F Return code from control block token validation processing

10–17 Address of the associated control block. For PCIR records, this is the PFCTE. For PCII records, this is the SLNCB.

18–1F The time stamp that is taken when the interrupt occurs

QSRB entry for Queue Service Request Block (SRB) events

Entry: QSRB

VIT option:
CIA

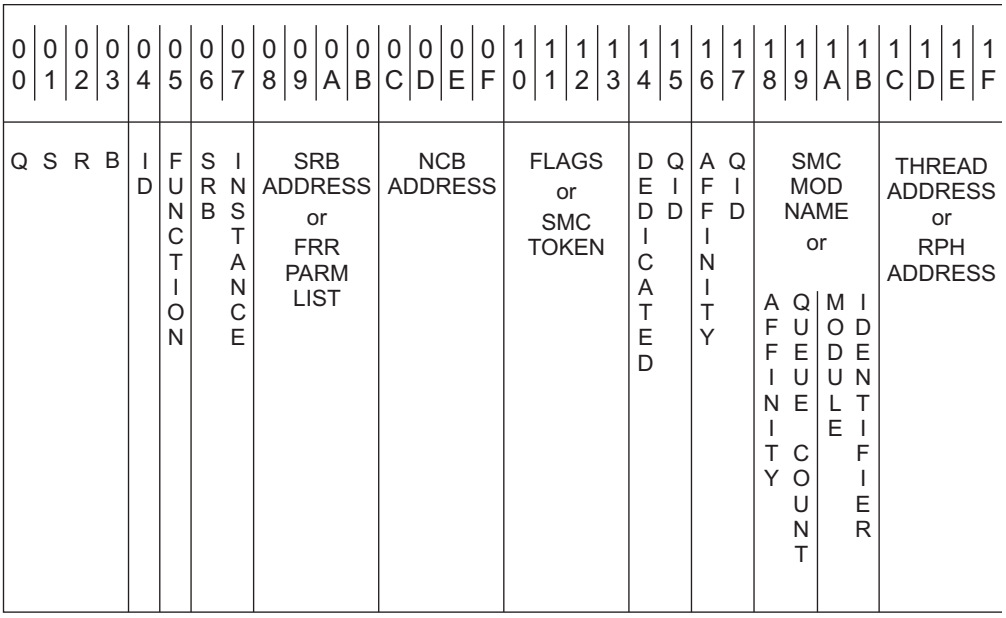
Subtrace Type:
DIO

Event: Schedule, dispatch, return, or exit of an SRB that is associated with the OSA-Express QDIO, Shared Memory Communications over Remote Direct Memory Access (SMC-R), Shared Memory Communications - Direct Memory Access (SMC-D), or a HiperSockets read operation

VIT processing module:
ISTITCOD

Control is returned to:
IUTLLCIE, ISTLLCWC, IUTLLCDQ, ISTSRIDQ, ISTSICDQ

This trace record is written to show the scheduling, dispatching, returning, and exiting of inbound OSA-Express QDIO, SMC-R, SMC-D, or HiperSockets processing.



Byte (hex)
Contents

00–03 Record ID: C"QSRB"

04 ID is the primary address space ID (ASID). This field is 0 if the ASID is greater than X'FF'.

05 Function:

- C"D" for Dispatch
- C"E" for Exit
- C"R" for Return to IUTLLCD
- C"S" for Schedule

06–07 SRB instance field that is used to correlate QSRB events

08–0B Service Request Block (SRB) address or FRR parameter list address

- If bytes 18–19 are 'SR' or 'SI', this is the FRR parameter list address for function Dispatch, and 0 for all other functions.
- Otherwise, this is the SRB address.

0C–0F NCB address that is associated with this SRB event

- If bytes 18–19 are 'SR', this is an RUNCB address
- If bytes 18–19 are 'SI', this is an SLNCB address
- Otherwise, this is a DINCB address

10–13 If bytes 18–19 are not 'SR' or 'SI', this field contains processing flags. See the *proc_flags* definitions in the module that is identified by bytes 1A-1B.

If bytes 18–19 are 'SR' or 'SI', this field contains the input token that is related to the SMC-R event.

14–15 Dedicated queue identifier, or zeros if bytes 18–19 are 'SR' or 'SI'.

16–17 Affinity queue identifier, or zeros if bytes 18–19 are 'SR' or 'SI'.

18–1B If this event is associated with an SMC-R event, this field is a 4-character module identifier, where the first 2 characters are 'SR'.

If this event is associated with an SMC-D event, this field is a 4-character module identifier, where the first 2 characters are 'SI'.Otherwise:

- Bytes 18–19 are the affinity queue element count, or zeros if bytes 16–17 are zeros.
- Bytes 1A-1B are a 2-character module identifier for the module that issued the INTRACE.

1C–1F Request parameter header (RPH) address.

RPST entry for invoking a RoCE Post command (Part 1)

Entry: RPST

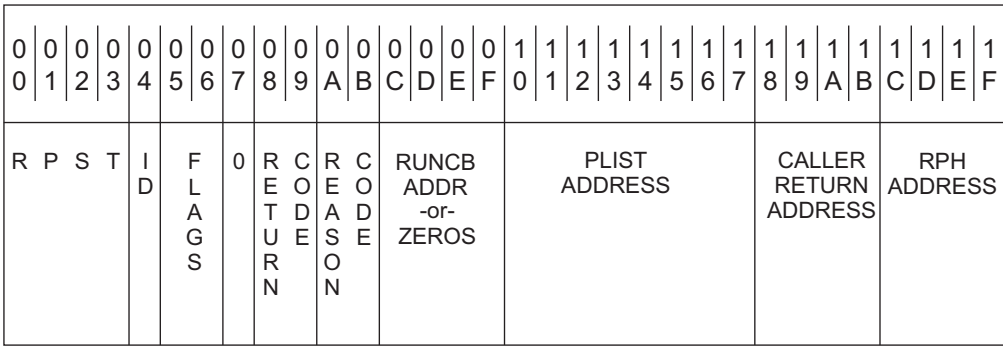
VIT option:
CIA

Event: Invocation of a Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) Post command, as part of Shared Memory Communications over Remote Direct Memory Access (SMC-R) processing.

VIT processing module:
ISTITCSH

Control is returned to:
The module that issued the INTRACE macroinstruction

This trace record is written upon completion of a RoCE Post operation.



Byte (hex)
Contents

00–03 Record ID: C'RPST'

04 ID is the primary address space ID (ASID). This field is 0 if the ASID is greater than X'FF'.

05–06 Option and output flags

07 0

08–09 Return code from the Post operation

0A–0B Reason code

0C–0F Address of the associated RUNCB

10–17 Parameter list address

18–1B Return address of the calling routine

1C–1F Request parameter header (RPH) address

RPSA entry for invoking a RoCE Post command (Part 3)

Entry: RPSA

VIT option:
CIA

Event: Invocation of a Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) Post command, as part of Shared Memory Communications over Remote Direct Memory Access (SMC-R) processing.

VIT processing module:
ISTITCSH

This trace record is continuation of the RPST record. Multiple RPSA entries can be generated, one for each array entry that was provided as input on the Post command.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
R	P	S	A	TYPE	0	WQE		USER DATA								BYTE COUNT				LKEY				0				IMMED DATA or TIMER CONTROL			

Byte (hex)
Contents

00–03 Record ID: C'RPSA'

04 Post operation type
- I for Send Immediate operation
- M for RDMA Write Immediate operation
- W for RMDA Write operation
- S for Send operation

05 0

06–07 Work Queue Element (WQE) number that is associated with this array entry

08–0F UserData that is associated with this Post operation

10–13 Amount of data to be sent on this Post operation

14–17 Local Key (LKEY) of the source buffer or 0:
- If Post operation type is 'M' or 'W', the Local Key (LKEY) of the source buffer
- Otherwise, 0

18–1B 0

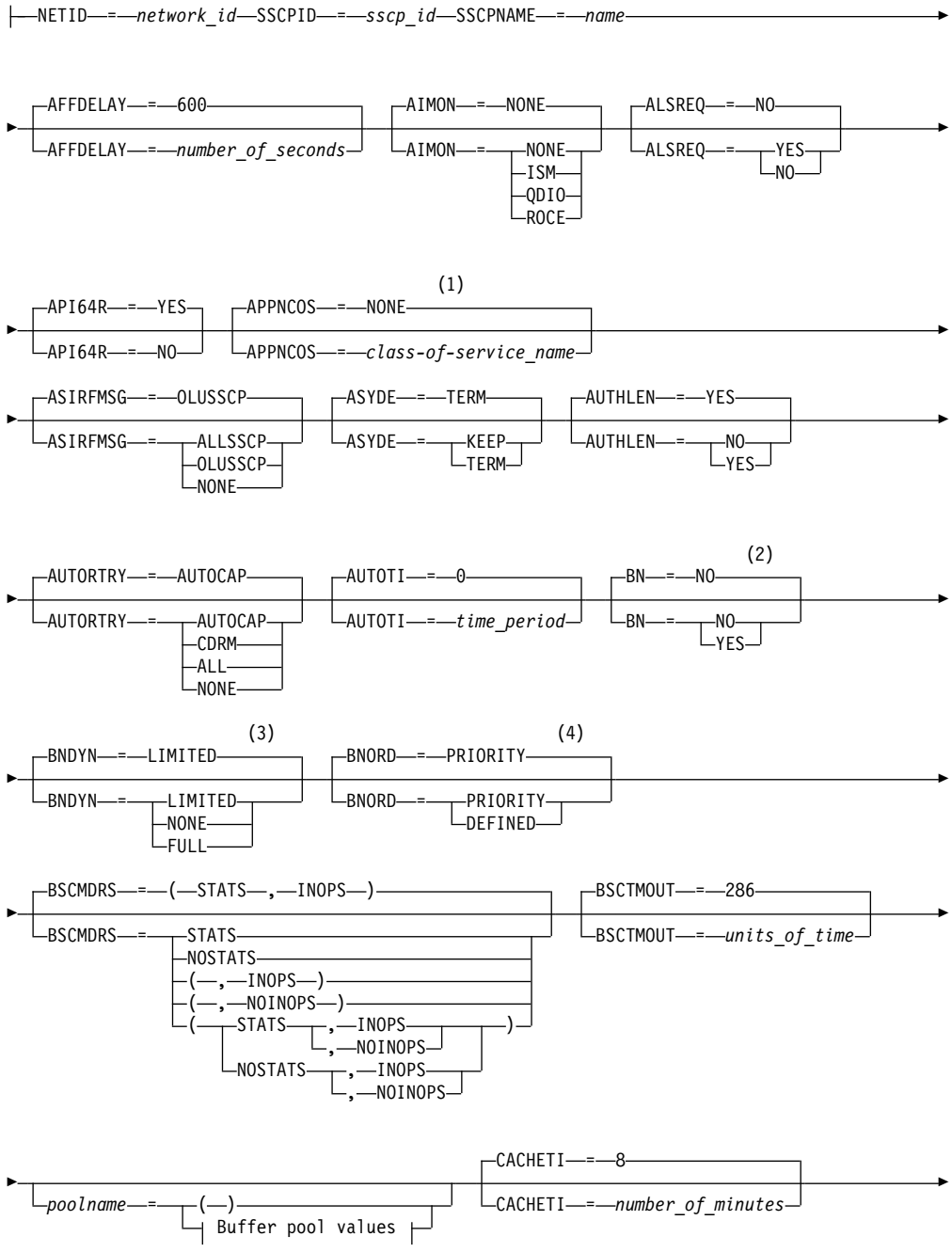
1C–1F

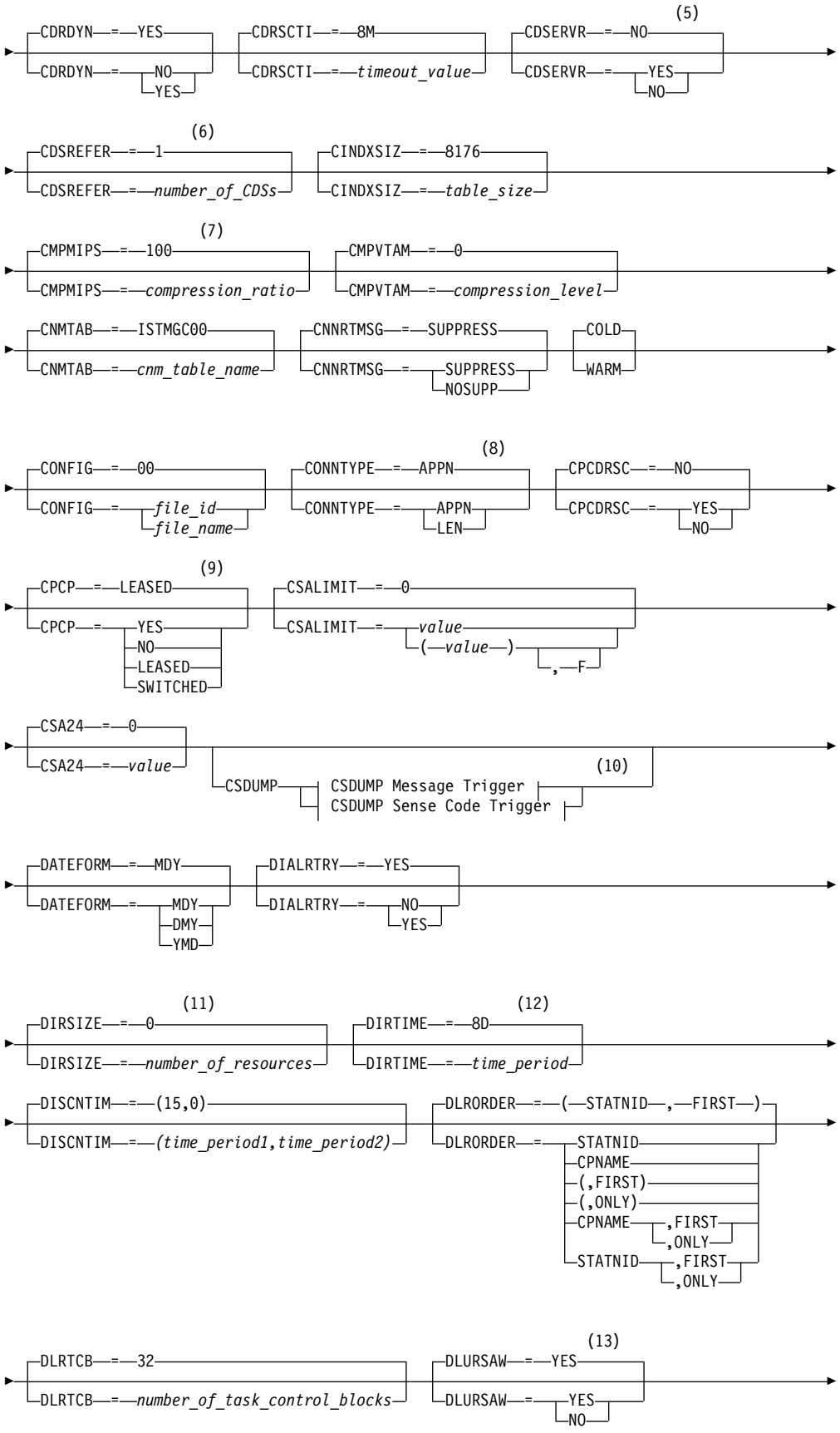
- If Post operation is 'I' or 'M', immediate data to be sent as part of this Post operation
- If Post operation is 'S', write completion timer control field
- Otherwise, 0

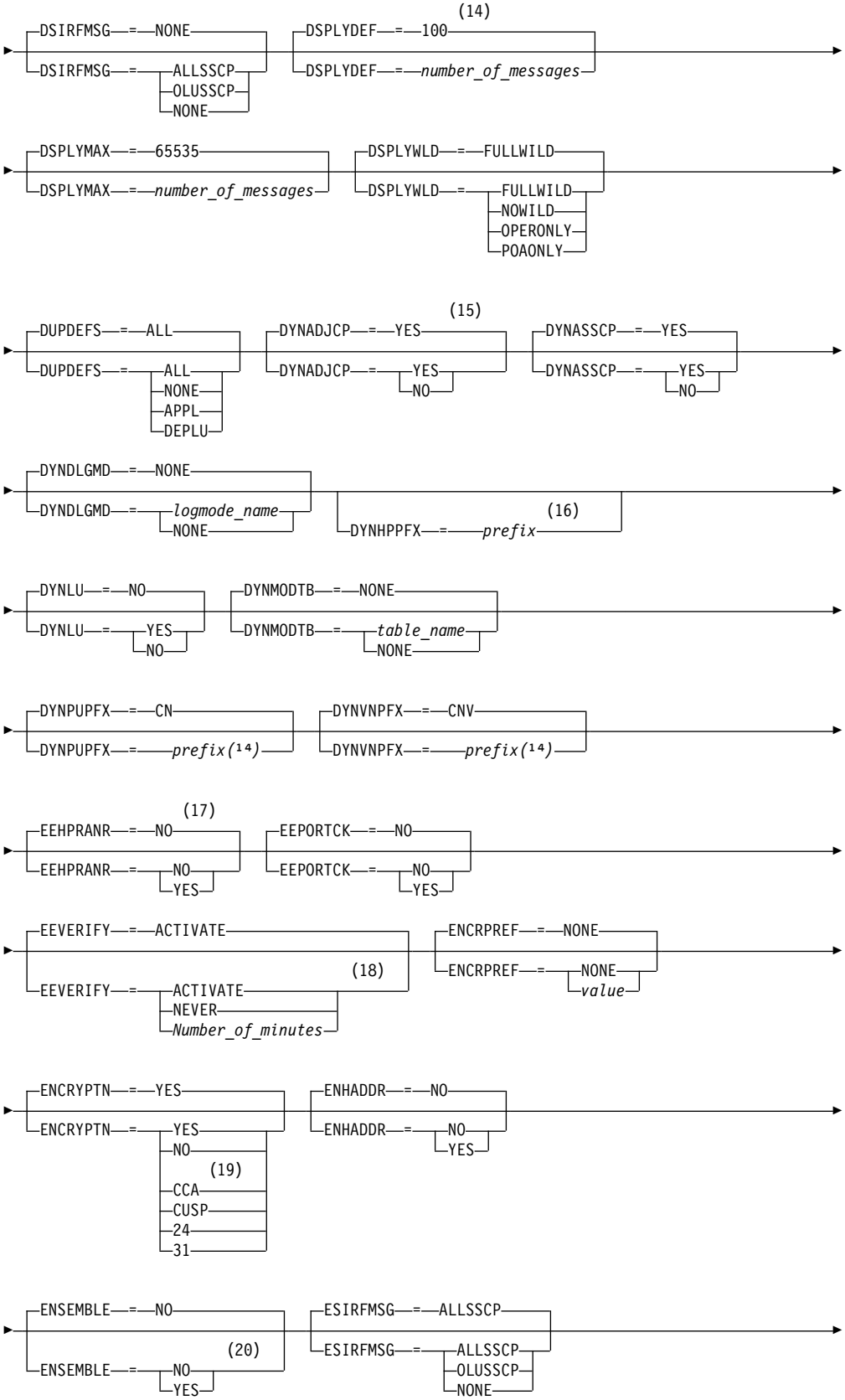
Chapter 12. SNA Resource Definition Reference

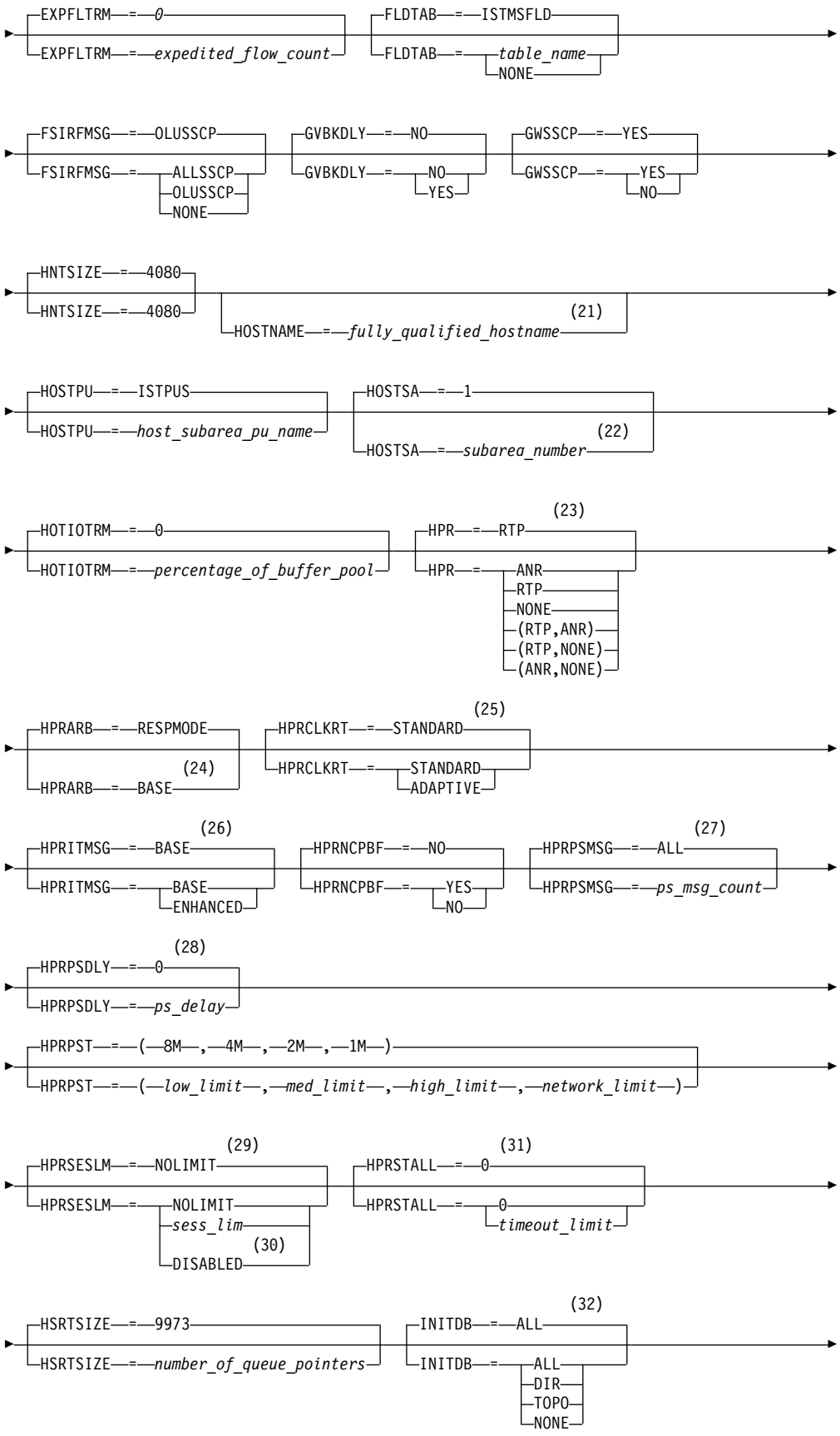
Start options syntax diagrams

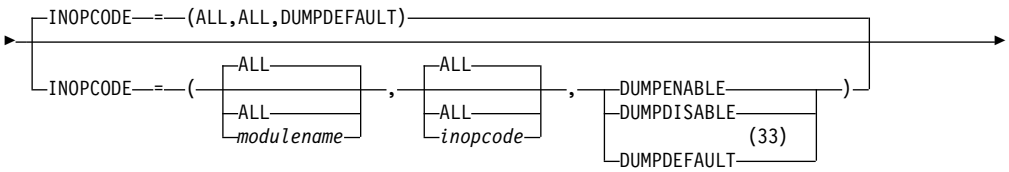
Options:

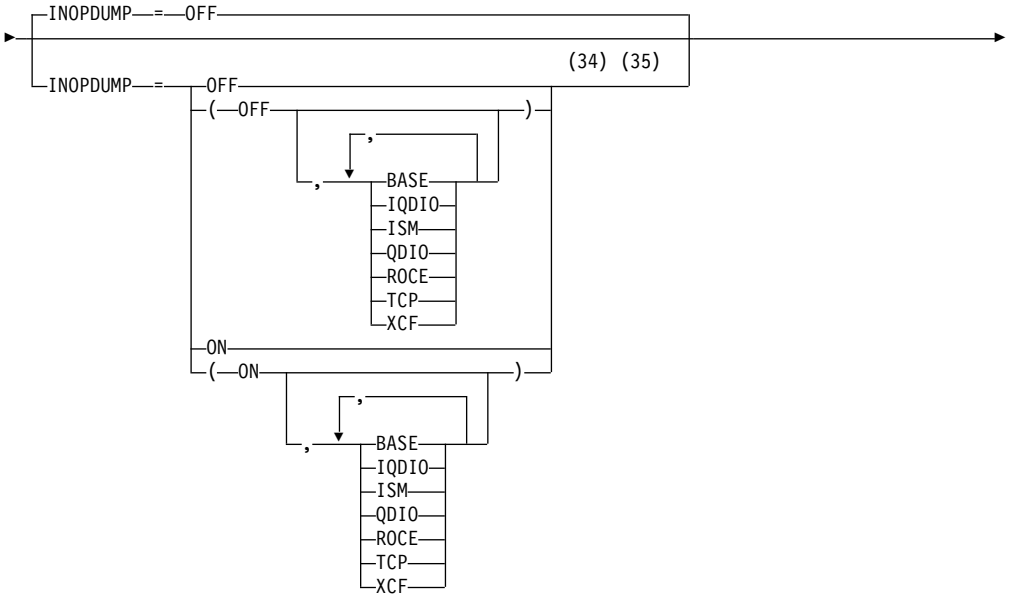


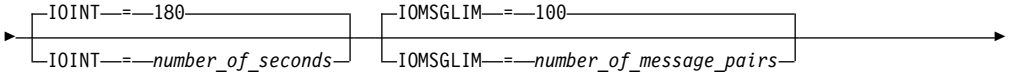

CDRDYN = YES
CDRDYN = NO
YES
CDRSCTI = 8M
CDRSCTI = timeout_value
(5)
CDSERVR = NO
CDSERVR = YES
NO
(6)
CDSREFER = 1
CDSREFER = number_of_CDSs
CINDXSIZ = 8176
CINDXSIZ = table_size
(7)
CMPMIPS = 100
CMPMIPS = compression_ratio
CMPVTAM = 0
CMPVTAM = compression_level
CNMTAB = ISTMGC00
CNMTAB = cnm_table_name
CNNRTMSG = SUPPRESS
CNNRTMSG = SUPPRESS
NOSUPP
COLD
WARM
CONFIG = 00
CONFIG = file_id
file_name
(8)
CONNTYPE = APPN
CONNTYPE = APPN
LEN
CPCDRSC = NO
CPCDRSC = YES
NO
(9)
CPCP = LEASED
CPCP = YES
NO
LEASED
SWITCHED
CSALIMIT = 0
CSALIMIT = value
(value)
, F
CSA24 = 0
CSA24 = value
CSDUMP
CSDUMP Message Trigger
CSDUMP Sense Code Trigger
(10)
DATEFORM = MDY
DATEFORM = MDY
DMY
YMD
DIALRTRY = YES
DIALRTRY = NO
YES
(11)
DIRSIZE = 0
DIRSIZE = number_of_resources
(12)
DIRTIME = 8D
DIRTIME = time_period
DISCNTIM = (15,0)
DISCNTIM = (time_period1,time_period2)
DLRORDER = (STATNID , FIRST)
DLRORDER = STATNID
CPNAME
(,FIRST)
(,ONLY)
CPNAME ,FIRST
,ONLY
STATNID ,FIRST
,ONLY
DLRTCB = 32
DLRTCB = number_of_task_control_blocks
(13)
DLURSAW = YES
DLURSAW = YES
NO

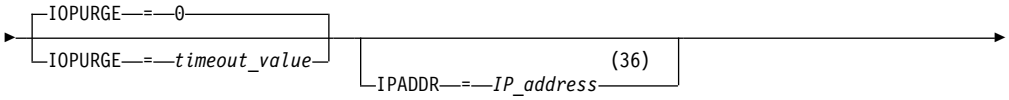

DSIRFMSG=NONE
DSIRFMSG=ALLSSCP
OLUSSCP
NONE
(14)
DSPLYDEF=100
DSPLYDEF=number_of_messages
DSPLYMAX=65535
DSPLYMAX=number_of_messages
DSPLYWLD=FULLWILD
DSPLYWLD=FULLWILD
NOWILD
OPERONLY
POAONLY
DUPDEFS=ALL
DUPDEFS=ALL
NONE
APPL
DEPLU
(15)
DYNADJCP=YES
DYNADJCP=YES
NO
DYNASSCP=YES
DYNASSCP=YES
NO
DYNDLGMD=NONE
DYNDLGMD=logmode_name
NONE
(16)
DYNHPPFX=prefix
DYNLU=NO
DYNLU=YES
NO
DYNMODTB=NONE
DYNMODTB=table_name
NONE
DYNPUPFX=CN
DYNPUPFX=prefix(14)
DYNVNPFX=CNV
DYNVNPFX=prefix(14)
(17)
EEHPRANR=NO
EEHPRANR=NO
YES
EEPORTCK=NO
EEPORTCK=NO
YES
EEVERIFY=ACTIVATE
EEVERIFY=ACTIVATE
NEVER
Number_of_minutes
(18)
ENCRPREF=NONE
ENCRPREF=NONE
value
ENCRYPTN=YES
ENCRYPTN=YES
NO
CCA
CUSP
24
31
(19)
ENHADDR=NO
ENHADDR=NO
YES
ENSEMBLE=NO
ENSEMBLE=NO
YES
(20)
ESIRFMSG=ALLSSCP
ESIRFMSG=ALLSSCP
OLUSSCP
NONE

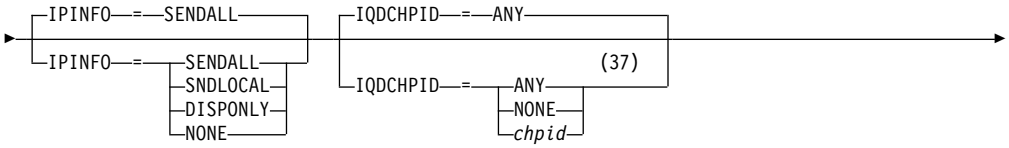

EXPFLTRM
=
0
expedited_flow_count
FLDTAB
=
ISTMSFLD
table_name
NONE
FSIRFMSG
=
OLUSSCP
ALLSSCP
OLUSSCP
NONE
GVBKDLY
=
NO
YES
GWSSCP
=
YES
NO
HNTSIZE
=
4080
HOSTNAME
=
fully_qualified_hostname
(21)
HOSTPU
=
ISTPUS
host_subarea_pu_name
HOSTSA
=
1
subarea_number
(22)
HOTIOTRM
=
0
percentage_of_buffer_pool
HPR
=
RTP
ANR
RTP
NONE
(RTP,ANR)
(RTP,NONE)
(ANR,NONE)
(23)
HPRARB
=
RESPMODE
BASE
(24)
HPRCLKRT
=
STANDARD
ADAPTIVE
(25)
HPRITMSG
=
BASE
ENHANCED
(26)
HPRNCPBF
=
NO
YES
HPRPSMSG
=
ALL
ps_msg_count
(27)
HPRPSDLY
=
0
ps_delay
(28)
HPRPST
=
(
8M
,
4M
,
2M
,
1M
)
low_limit
med_limit
high_limit
network_limit
HPRSESLM
=
NOLIMIT
sess_lim
DISABLED
(29)
(30)
HPRSTALL
=
0
timeout_limit
(31)
HSRTSIZE
=
9973
number_of_queue_pointers
INITDB
=
ALL
DIR
TOPO
NONE
(32)

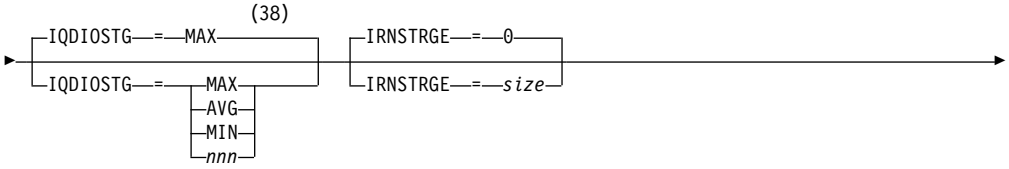

INOPCODE=(ALL,ALL,DUMPDEFAULT)
INOPCODE=(ALL,ALL,DUMPENABLE)
ALL
modulename
ALL
inopcode
DUMPDISABLE
DUMPDEFAULT
(33)

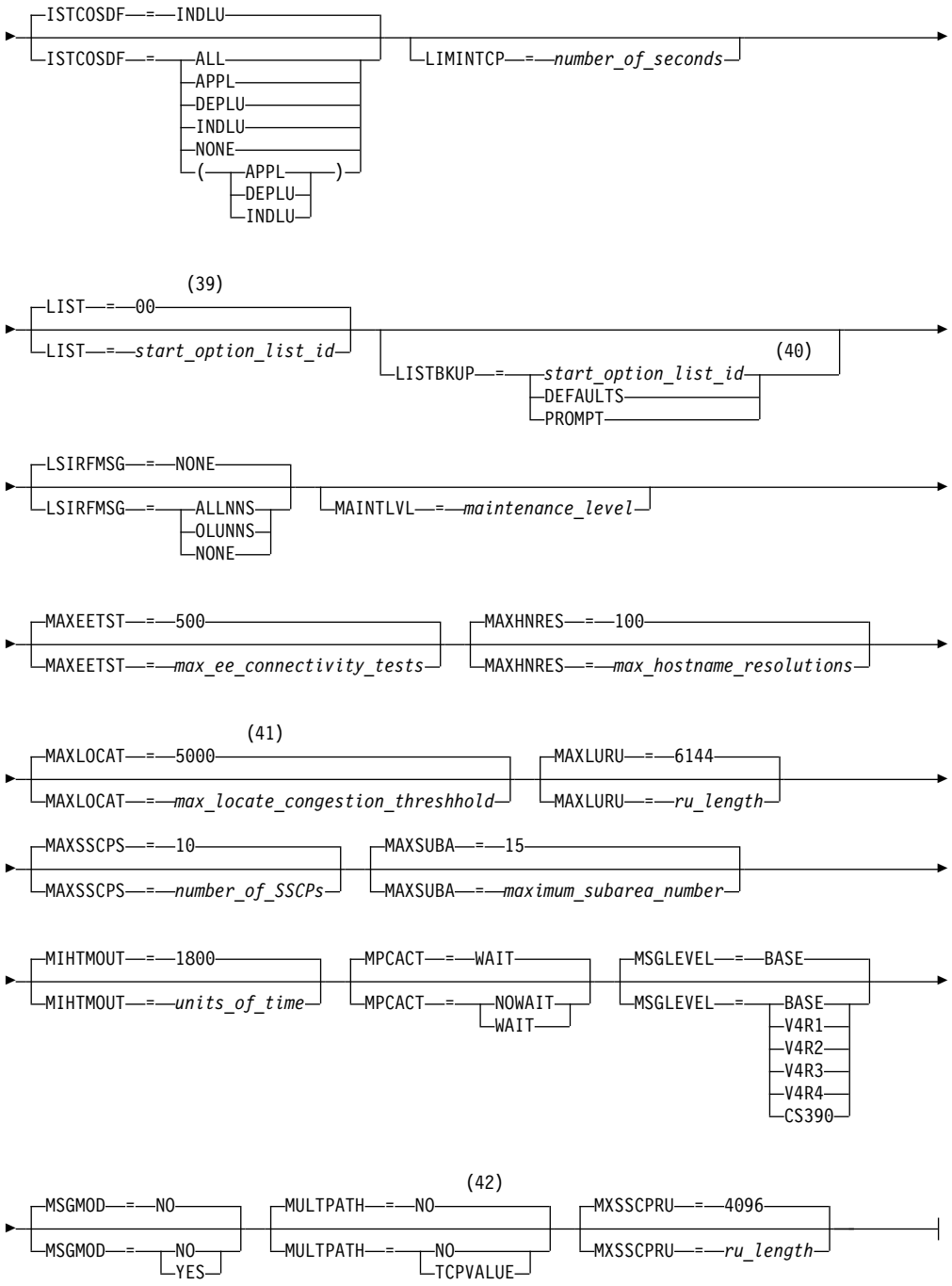

INOPDUMP=OFF
INOPDUMP=OFF
(34) (35)
(OFF)
BASE
IQDIO
ISM
QDIO
ROCE
TCP
XCF
ON
(ON)
BASE
IQDIO
ISM
QDIO
ROCE
TCP
XCF


IOINT=180
IOINT=number_of_seconds
IOMSGLIM=100
IOMSGLIM=number_of_message_pairs


IOPURGE=0
IOPURGE=timeout_value
IPADDR=IP_address
(36)


IPINFO=SENDALL
IPINFO=SENDALL
SNDLOCAL
DISPONLY
NONE
IQDCHPID=ANY
IQDCHPID=ANY
NONE
chpid
(37)


IQDIOSTG=MAX
IQDIOSTG=MAX
AVG
MIN
nnn
(38)
IRNSTRGE=0
IRNSTRGE=size



Notes:

1 APPNCOS is meaningful only if the NODETYPE start option is also used.

2 BN is meaningful only if the NODETYPE=NN start option is also used.

3 BNDYN is meaningful only if the BN=YES start option is also used.

4 BNORD is meaningful only if the BN=YES start option is also used.

5 CDSERVR is meaningful only if the NODETYPE=NN start option is also used.

6 CDSREFER is meaningful only if the NODETYPE=NN and CDSERVR=NO start options are also used.

7 The CMPMIPS start option is meaningful only if the value for CMPVTAM is greater than 1.

8 CONNTYPE is meaningful only if the NODETYPE start option is also used.

9 CPCP is meaningful only if the NODETYPE start option is also used.

10 Specify the CSDUMP start option twice to set both message and sense code triggers.

11 DIRSIZE is meaningful only if the NODETYPE=NN start option is also used.

12 DIRTIME is meaningful only if the NODETYPE=NN start option is also used.

13 DLURSAW is meaningful only if the NODETYPE=NN start option is also used.

14 If the DSPLYMAX start option value is less than 100, that value is the default for DSPLYDEF.

15 DYNADJCP is meaningful only if the NODETYPE start option is also used.

16 Two character prefix.

17 EEHPRANR is meaningful only when the NODETYPE=NN start option is also used.

18 The EEVERIFY start option is meaningful only if VTAM provides RTP-level HPR support. The NODETYPE start option must be coded and the RTP value must be specified on the HPR start option.

19 ENCRYPTN=CCA needs to be coded when Triple Des Encryption is desired.

20 The ENSEMBLE setting is used to either permit or deny connectivity to the intraensemble data network (IEDN) and the intranode management network (INMN) by allowing or denying activation of OSX and OSM interfaces.

21 HOSTNAME is meaningful only if the NODETYPE start option is also used.

22 HOSTSA specifies the subarea number of this VTAM. If HOSTSA is not coded, then a default subarea number of 1 is used.

23 HPR is meaningful only if NODETYPE is also used.

24 This start option was provided by APAR OW36113 for use in migration to VTAM V4R5. Do not use this option unless you use the default value of RESPMODE.

25 HPRCLKRT=ADAPTIVE is meaningful only for Enterprise Extender configurations that have a defined capacity of 1 Gb or higher access speeds.

26 This option is meaningful only if VTAM provides RTP-level HPR support.

27 This option is meaningful only if VTAM provides RTP-level HPR support.

28 This option is meaningful only if VTAM provides RTP-level HPR support.

29 This option is meaningful only if VTAM provides RTP-level HPR support.

30 HPRSESLM=DISABLED is meaningful only on interchange nodes.

31 This option is meaningful only if VTAM provides RTP-level HPR support.

32 INITDB is meaningful only if the NODETYPE=NN start option is also used.

33 INOPCODE has no effect unless INOPDUMP is active for the resource when an inoperative condition is detected.

34 INOPDUMP status is propagated to resources that are defined within a transport resource list entry when the entry is activated.

35 The INOPCODE start option provides more granular control of the INOPDUMP function. Refer to the INOPCODE in this section and the DISPLAY INOPCODE command in z/OS Communications Server: SNA Operation for additional details.

36 IPADDR is meaningful only if the NODETYPE start option is also used.

37 The IQDCHPID option controls which IQD CHPID (and related subchannel devices) VTAM selects to dynamically build the iQDIO (IUTIQDIO) MPC group. The IUTIQDIO MPC group is used for TCP/IP dynamic XCF communications within this System z system. Although this option can be modified (and the modification will immediately be displayed) while the IUTIQDIO MPC group is currently active, any modifications will have the effects: 1) Modified from ANY (or CHPID) to NONE has no effect on current usage but blocks subsequent activations; 2) Modified from NONE to ANY (or CHPID) has no effect on current usage but allows subsequent activations; 3) Modified from CHPID_X to CHPID_Y has no effect on current usage. VTAM only uses the CHPID value when building the IUTIQDIO MPC group. To change CHPIDs for an active MPC group, the steps must be done: 1) All TCP/IP iQDIO (HiperSockets) devices must be stopped; 2) Make any necessary HCD/IOCDS changes; 3) Verify that new subchannel devices are varied online; 4) Verify that the MPC group has deactivated (with no usage, it times out after approximately two minutes); 5) Modify IQDCHPID=*chpid* (to new CHPID); 6) Restart the TCP/IP iQDIO device or devices. In order to use iQDIO communications, the processor must have the necessary hardware support. If the processor does not support iQDIO communications, then modifications to this start option will not be accepted and the IQDCHPID option will not be displayed (displayed as ***NA***).

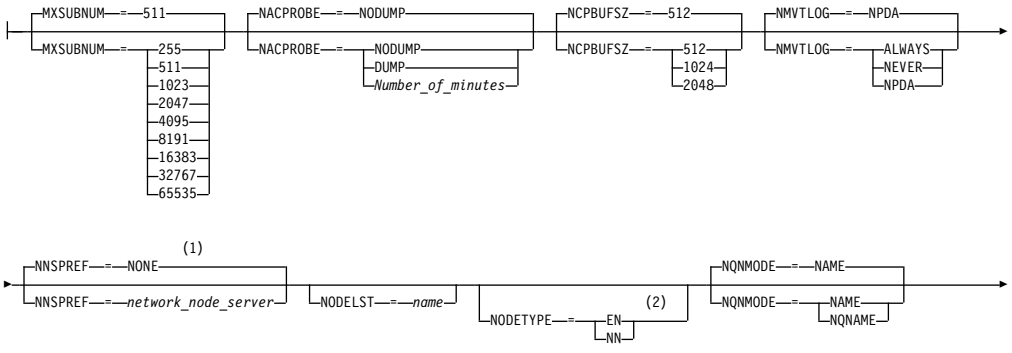
38 This option only affects iQDIO devices that use a MFS of 64k. The smaller frame sizes will always use 126 SBALs.

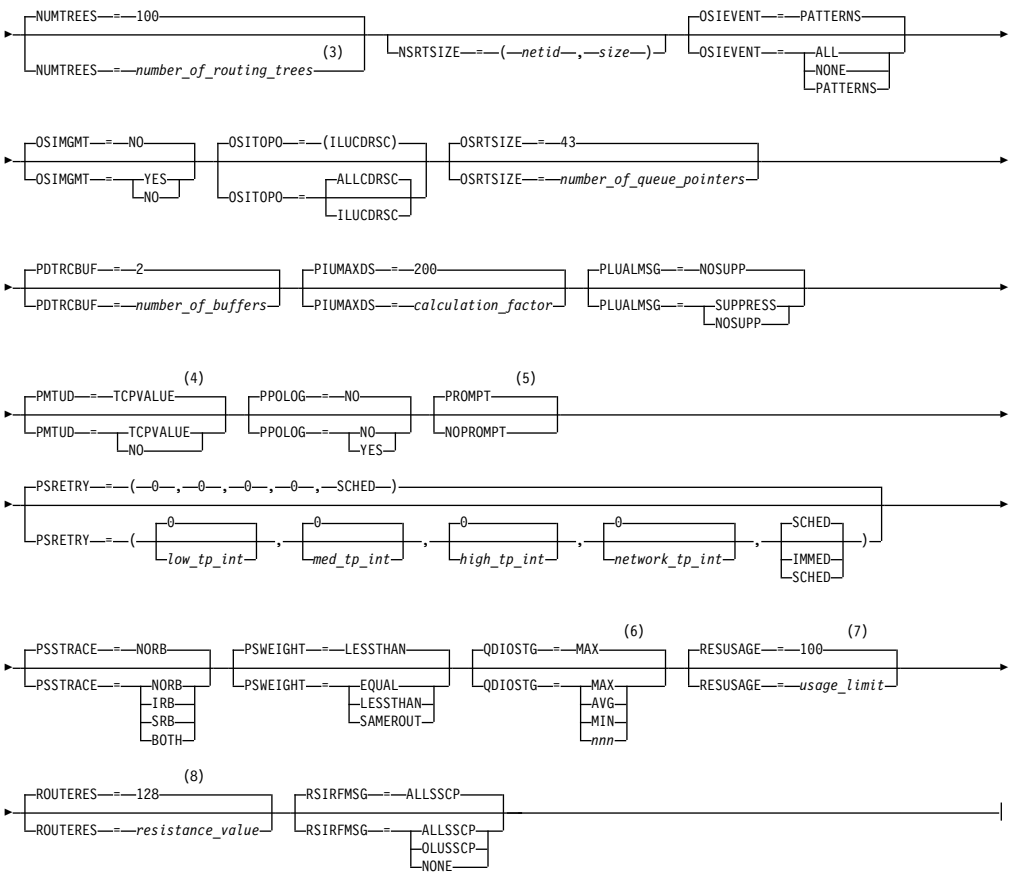
39 LIST can be entered by a VTAM operator only. If LIST is coded in an ATCSTR*xx* file, it is considered to be an error and is ignored.

40 LISTBKUP can be coded in a start option file only. If you enter it on the START command or at an operator prompt, VTAM will ignore it.

41 MAXLOCAT is meaningful only if NODETYPE is specified.

42 MULTPATH is meaningful only if the NODETYPE start option is also specified.





Notes:

1 NNSPREF can be specified only if NODETYPE=EN is specified during VTAM START processing.

2 NODETYPE enables APPN function. The combination of HOSTSA, NODETYPE, and SACONNS determines the configuration (subarea node, interchange node, migration data host, network node, or end node).

3 NUMTREES is meaningful only if the NODETYPE=NN start option is also used.

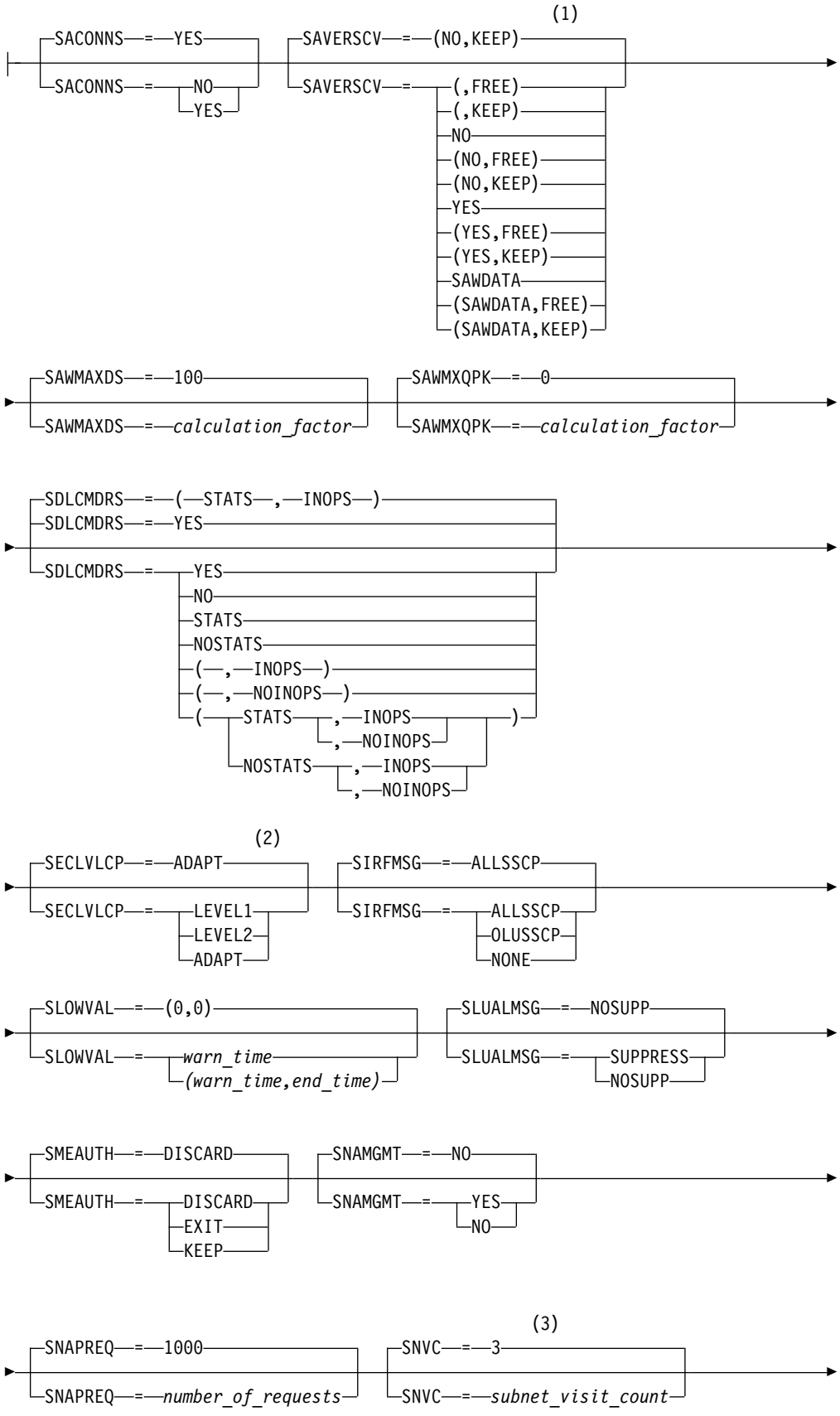
4 PMTUD is meaningful only if the NODETYPE start option is also used.

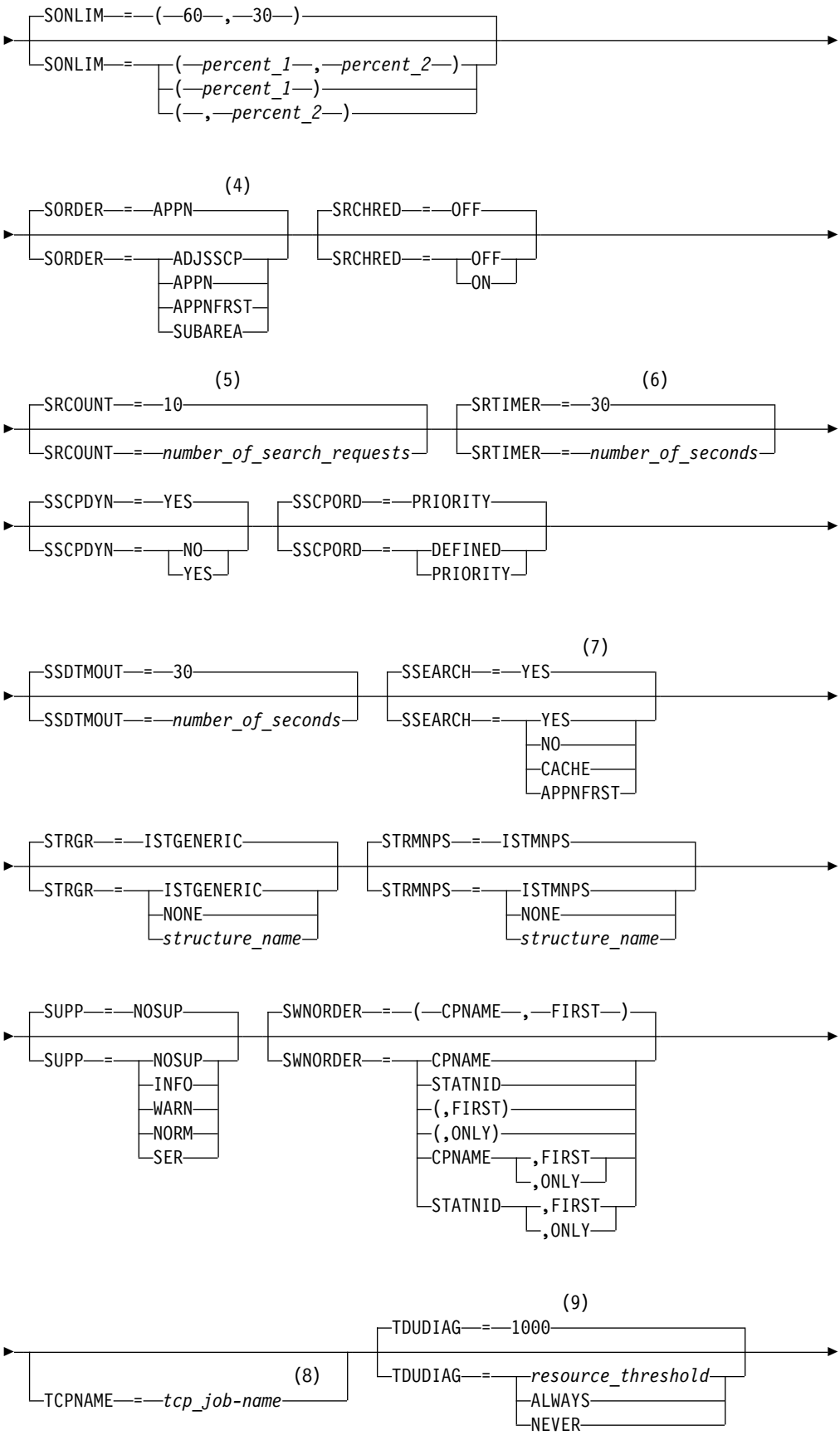
5 A VTAM operator cannot enter the PROMPT or NOPROMPT start option; it can be coded only in ATCSTR00. The value coded in ATCSTR00 is ignored if start options are entered on the START command or if VTAM finds an error in a start list. Upon finding an error in a start list, VTAM prompts the operator so that the operator can specify the option correctly.

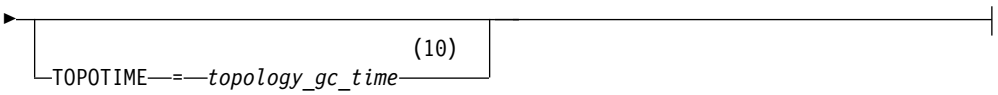
6 QDIOSTG defaults to MAX for 64-bit (z/Architecture) machines and MIN for non 64-bit machines.

7 RESUSAGE is meaningful only if the NODETYPE=NN start option is also used.

8 ROUTERES is meaningful only if the NODETYPE=NN start option is also used.


(1)
SACONNS=YES
SACONNS=NO
YES
SAVERSCV=(NO,KEEP)
SAVERSCV=(,FREE)
(,KEEP)
NO
(NO,FREE)
(NO,KEEP)
YES
(YES,FREE)
(YES,KEEP)
SAWDATA
(SAWDATA,FREE)
(SAWDATA,KEEP)
SAWMAXDS=100
SAWMAXDS=calculation_factor
SAWMXQPK=0
SAWMXQPK=calculation_factor
SDLCMDRS=(STATS,INOPS)
SDLCMDRS=YES
SDLCMDRS=YES
NO
STATS
NOSTATS
(,INOPS)
(,NOINOPS)
(STATS,INOPS)
(STATS,NOINOPS)
(NOSTATS,INOPS)
(NOSTATS,NOINOPS)
(2)
SECLVLCP=ADAPT
SECLVLCP=LEVEL1
LEVEL2
ADAPT
SIRFMSG=ALLSSCP
SIRFMSG=ALLSSCP
OLUSSCP
NONE
SLOWVAL=(0,0)
SLOWVAL=warn_time
(warn_time,end_time)
SLUALMSG=NOSUPP
SLUALMSG=SUPPRESS
NOSUPP
SMEAUTH=DISCARD
SMEAUTH=DISCARD
EXIT
KEEP
SNAMGMT=NO
SNAMGMT=YES
NO
(3)
SNAPREQ=1000
SNAPREQ=number_of_requests
SNVC=3
SNVC=subnet_visit_count


SONLIM=(60,30)
SONLIM=(percent_1,percent_2)
(percent_1)
(,percent_2)
(4)
SORDER=APPN
SORDER=ADJSSCP
APPN
APPNFRST
SUBAREA
SRCHRED=OFF
SRCHRED=OFF
ON
(5)
SRCOUNT=10
SRCOUNT=number_of_search_requests
(6)
SRTIMER=30
SRTIMER=number_of_seconds
SSCPDYN=YES
SSCPDYN=NO
YES
SSCPORD=PRIORITY
SSCPORD=DEFINED
PRIORITY
SSDTMOUT=30
SSDTMOUT=number_of_seconds
(7)
SSEARCH=YES
SSEARCH=YES
NO
CACHE
APPNFRST
STRGR=ISTGENERIC
STRGR=ISTGENERIC
NONE
structure_name
STRMNPS=ISTMNPS
STRMNPS=ISTMNPS
NONE
structure_name
SUPP=NOSUP
SUPP=NOSUP
INFO
WARN
NORM
SER
SWNORDER=(CPNAME,FIRST)
SWNORDER=CPNAME
STATNID
(,FIRST)
(,ONLY)
CPNAME,FIRST
,ONLY
STATNID,FIRST
,ONLY
(9)
TDUDIAG=1000
TDUDIAG=resource_threshold
ALWAYS
NEVER
(8)
TCPNAME=tcp_job-name



Notes:

1 SAVERSCV is meaningful only if NODETYPE is also used.

2 The SECLVLCP start option is meaningful only if the NODETYPE and VERIFYCP start options are also used.

3 SNVC is meaningful only if the BN=YES start option is also used.

4 SORDER is meaningful only in an interchange node or a migration data host.

5 SRCOUNT is meaningful only if the SRCHRED=ON start option is also used.

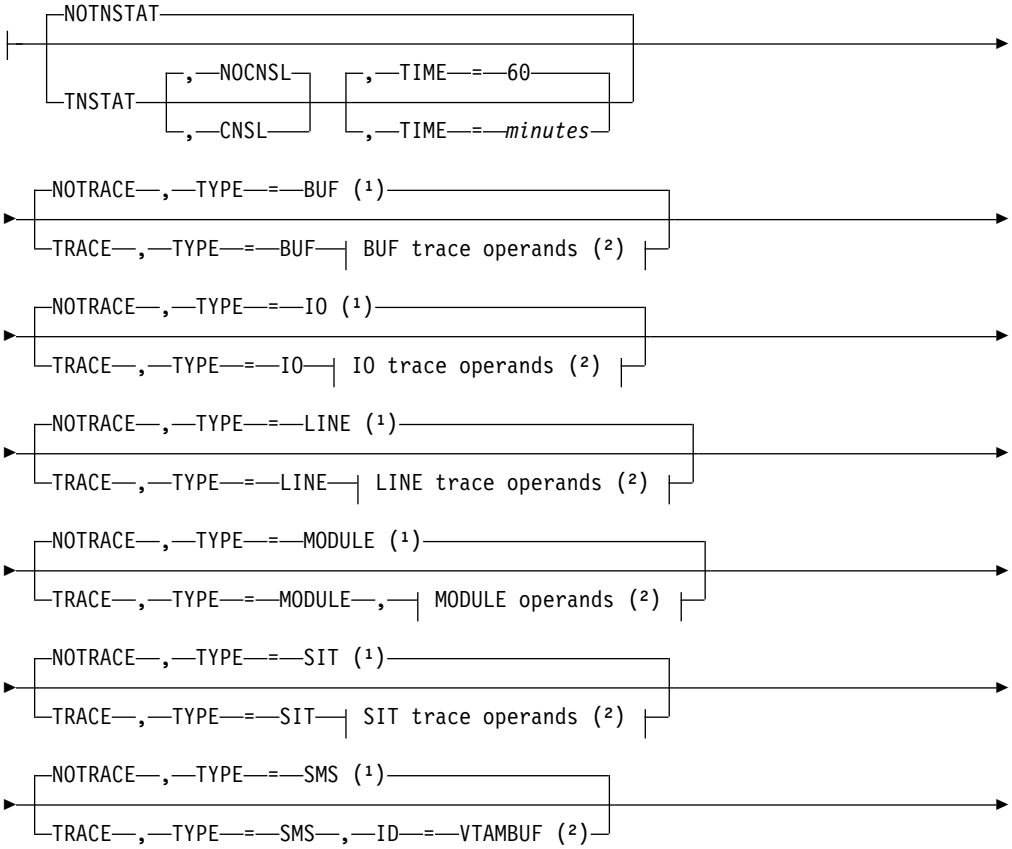
6 SRTIMER is meaningful only if the SRCHRED=ON start option is also used.

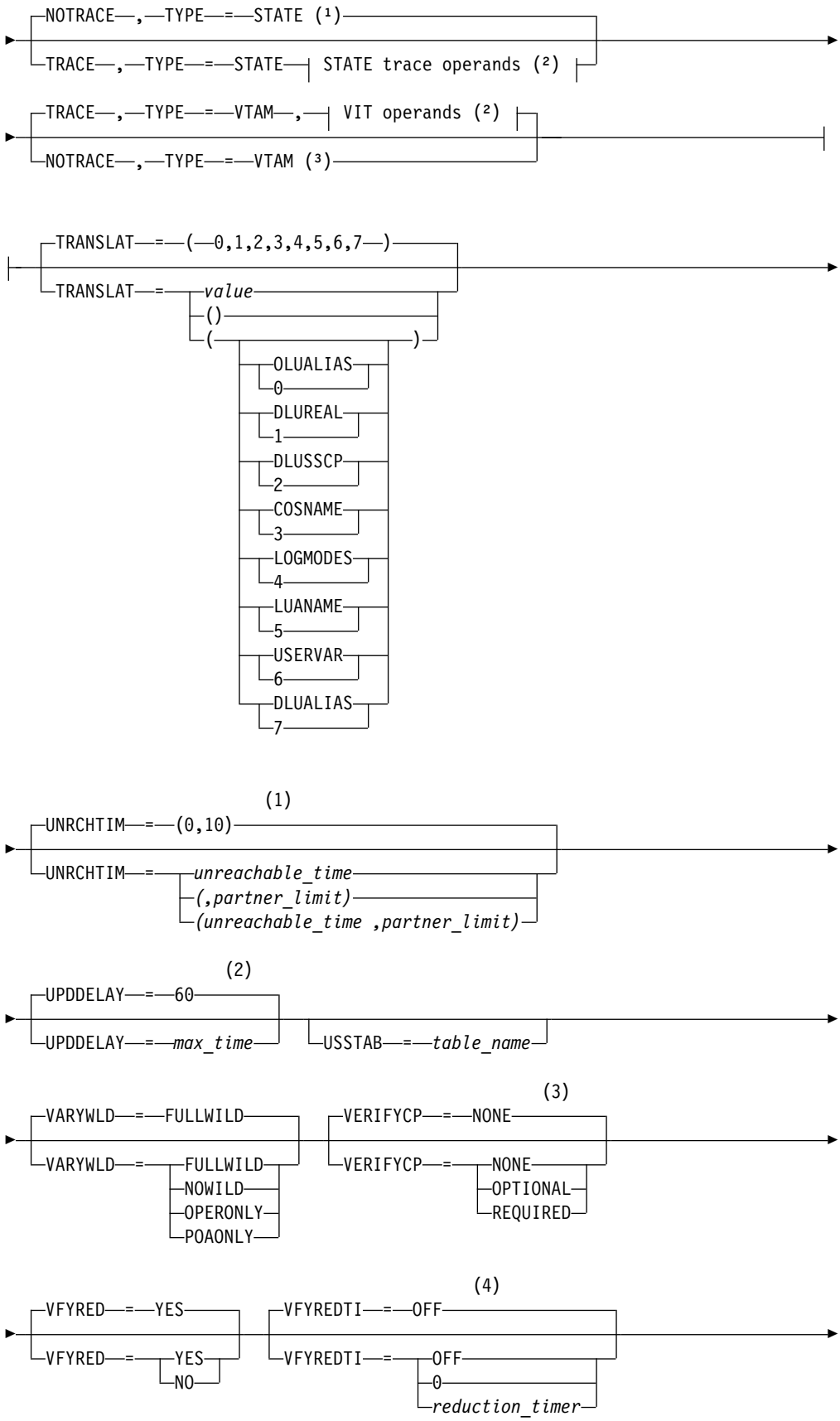
7 SSEARCH is meaningful only if the NODETYPE=NN start option is also used.

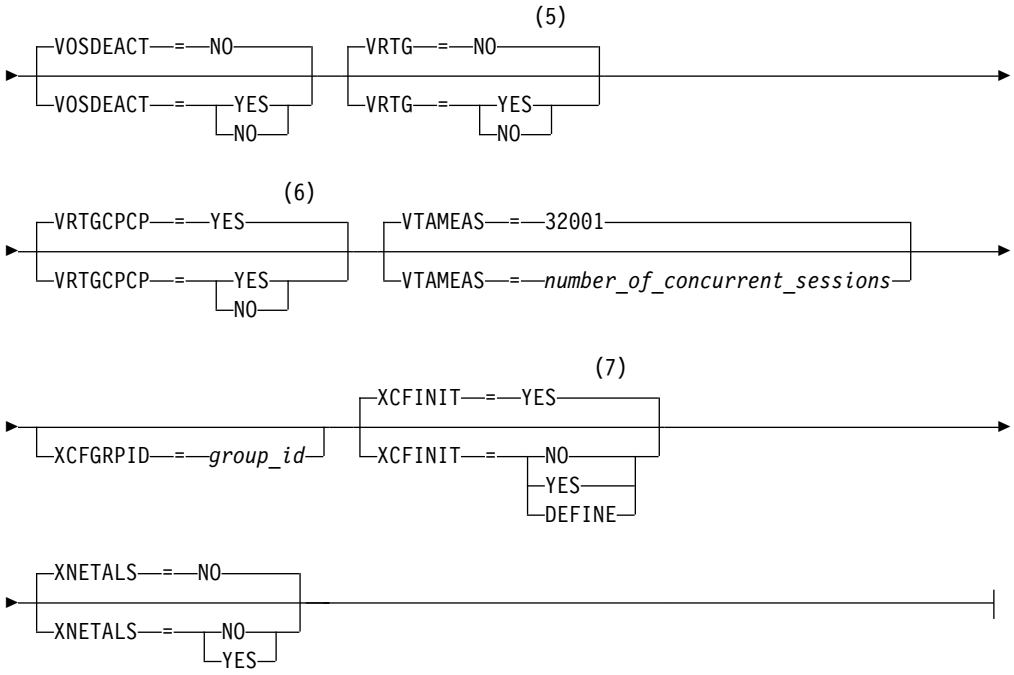
8 TCPNAME is meaningful only if the NODETYPE start option is also used.

9 TDUDIAG is meaningful only if the NODETYPE=NN start option is also being used.

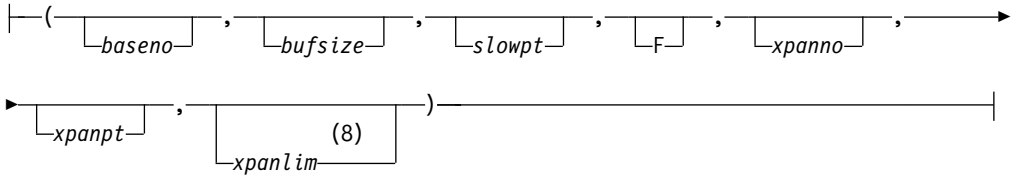
10 TOPOTIME is meaningful only if the NODETYPE start option is also used.



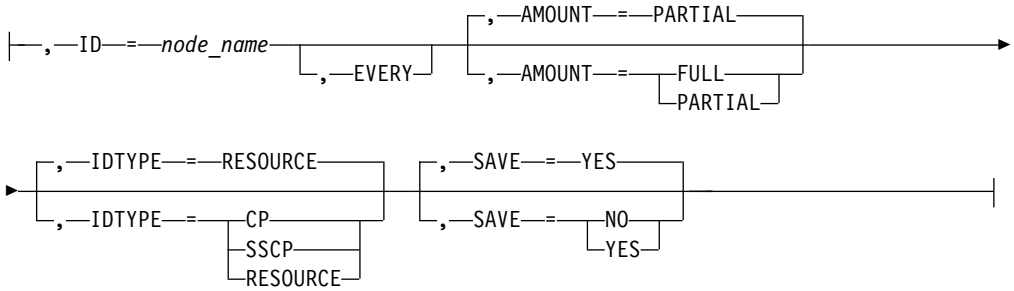

NOTRACE
,
TYPE
=
STATE (1)
TRACE
,
TYPE
=
STATE
STATE trace operands (2)
TRACE
,
TYPE
=
VTAM
,
VIT operands (2)
NOTRACE
,
TYPE
=
VTAM (3)
TRANSLAT
=
(
0,1,2,3,4,5,6,7
)
TRANSLAT
=
value
()
(
)
OLUALIAS
0
DLUREAL
1
DLUSSCP
2
COSNAME
3
LOGMODES
4
LUANAME
5
USERVAR
6
DLUALIAS
7
(1)
UNRCHTIM
=
(0,10)
UNRCHTIM
=
unreachable_time
(,partner_limit)
(unreachable_time ,partner_limit)
(2)
UPDDELAY
=
60
UPDDELAY
=
max_time
USSTAB
=
table_name
(3)
VARYWLD
=
FULLWILD
VARYWLD
=
FULLWILD
NOWILD
OPERONLY
POAONLY
VERIFYCP
=
NONE
VERIFYCP
=
NONE
OPTIONAL
REQUIRED
(4)
VFYRED
=
YES
VFYRED
=
YES
NO
VFYREDTI
=
OFF
VFYREDTI
=
OFF
0
reduction_timer



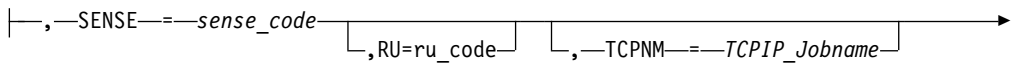
Buffer pool values:

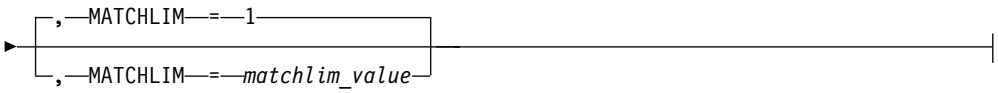


BUF trace operands:

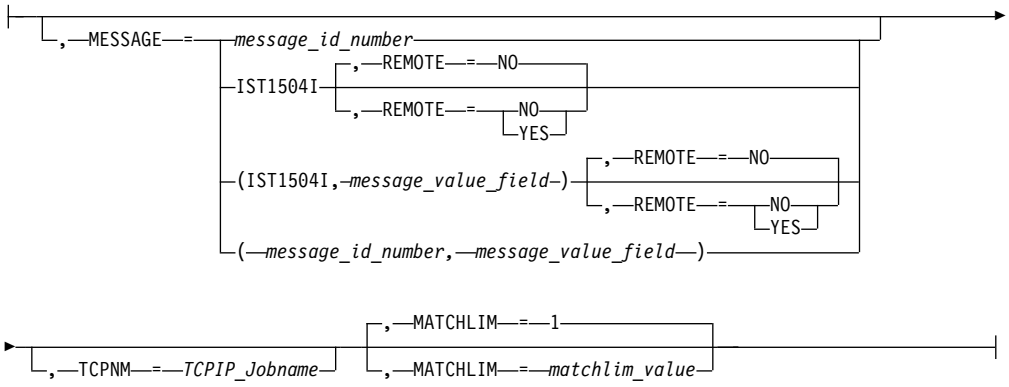


CSDUMP sense code trigger:

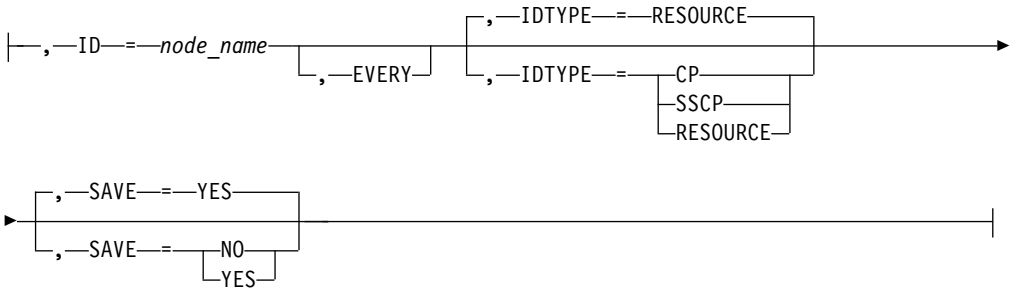




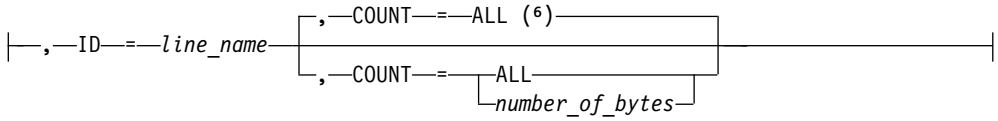
CSDUMP message trigger:



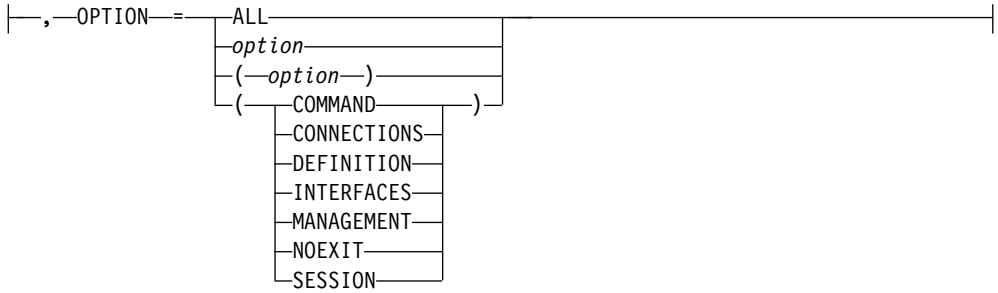
IO trace operands:



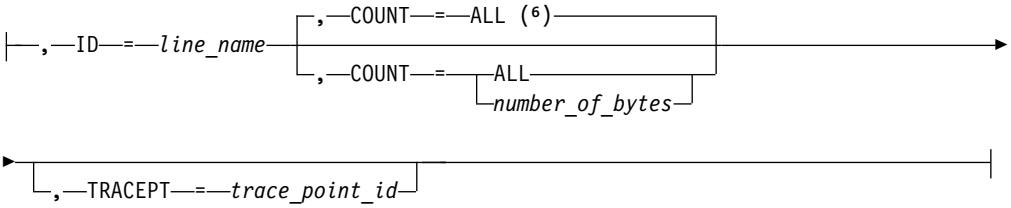
LINE trace operands:



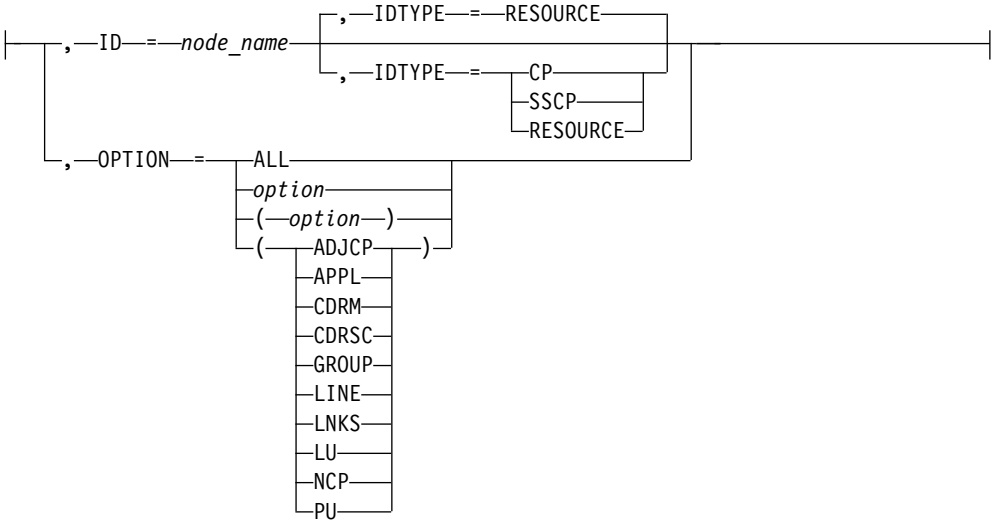
MODULE operands:



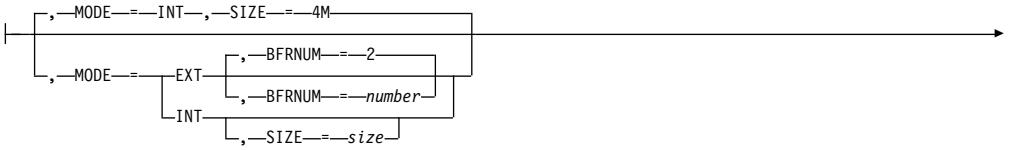
SIT trace operands:

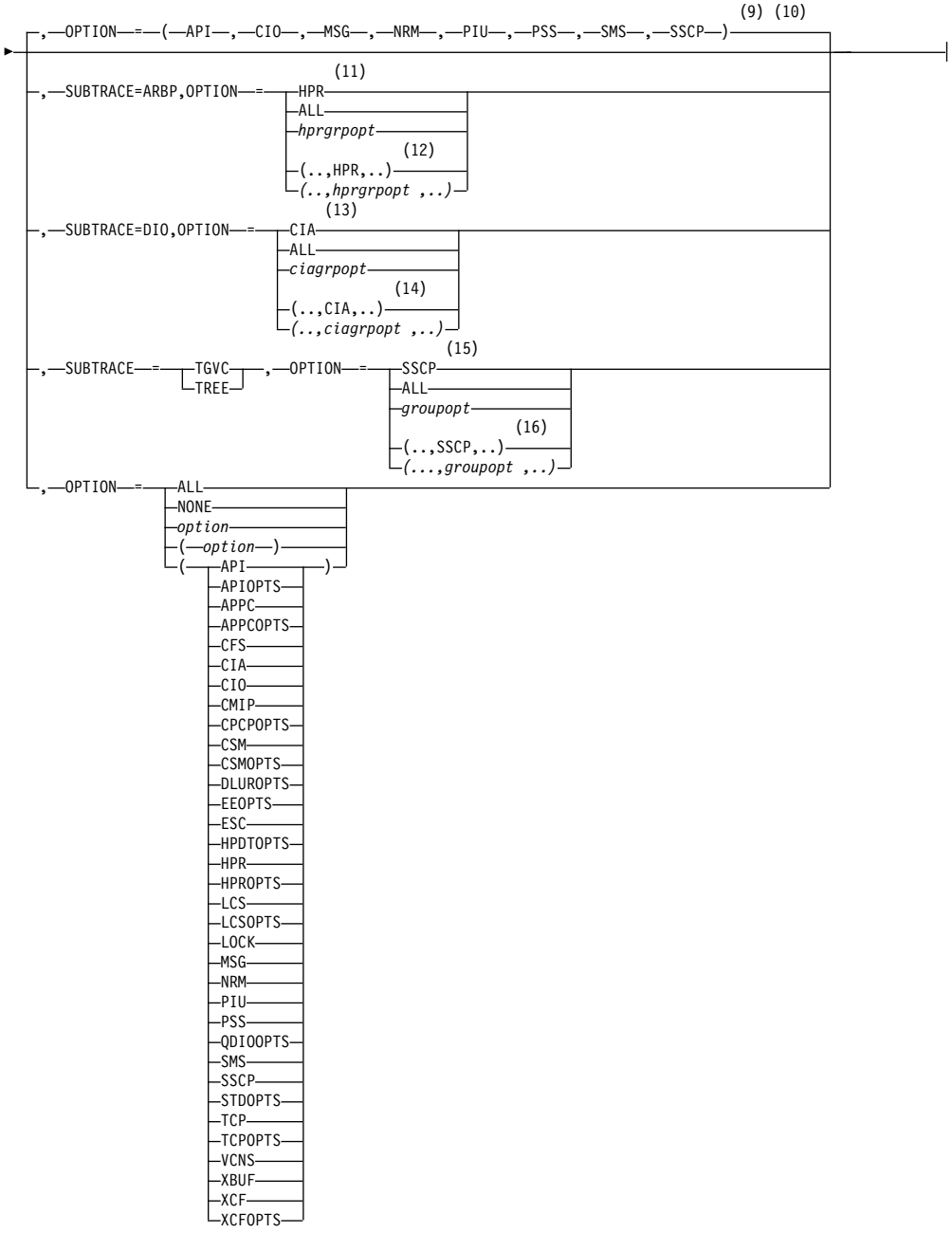


STATE trace operands:



VIT operands:





Notes:

1 UNRCHTIM is meaningful only if the NODETYPE start option is also used.

2 UPDDELAY is meaningful only if the OSIMGMT=YES start option is also used.

3 The VERIFYCP start option is meaningful only if the NODETYPE start option is also used.

4 VFYREDTI is meaningful only if the NODETYPE=NN start option is also used.

5 VRTG is meaningful only if the NODETYPE and HOSTSA start options are also used.

6 VRTGCPCP is meaningful only if the NODETYPE and HOSTSA start options are also used.

7 XCFINIT=YES is the default if VTAM is started as an APPN node (that is, the NODETYPE start option has been specified). XCFINIT=YES is not allowed for pure subarea nodes. XCFINIT=DEFINE is the default if VTAM is started as a pure subarea node (the NODETYPE start option has not been specified).

8 The IOBUF pool (IO00, IO) is the only buffer pool where all seven values can be specified. For all other buffer pools, the *xpanlim* field is not supported. If you specify the *xpanlim* field for any buffer pool other than the IOBUF pool (IO00, IO), even if the field is null, you get an IST1072I message.

9 The default options apply only to MODE=INT.

10 PSS and SMS can be turned off.

11 When SUBTRACE=ARBP is specified, if a single OPTION value is coded, it must be HPR, ALL, or one of the group options (*hprgrpopt*) that include HPR as an individual option equivalent. The applicable group options are DLUROPTS, EEOPTS, HPDTOPTS, HPROPTS, QDIOOPTS, and XCFOPTS.

12 If multiple trace options are coded in parentheses, either HPR or one of the group options (*hprgrpopt*) that include HPR as an individual option equivalent must be coded inside the parentheses when SUBTRACE=ARBP is coded.

13 When you specify SUBTRACE=DIO and you code a single OPTION value, the OPTION value must be CIA, ALL, or one of the group options (*ciagrpopt*) that include CIA as an individual option equivalent. The applicable group options are EEOPTS, HPDTOPTS, HPROPTS, QDIOOPTS, TCPOPTS and XCFOPTS.

14 When SUBTRACE=DIO is coded and you code multiple trace options in parentheses, you must code either CIA or one of the group options (*ciagrpopt*) that include CIA as an individual option equivalent inside the parentheses.

15 When SUBTRACE=TGVC or SUBTRACE=TREE is coded, if a single OPTION value is coded, it must be SSCP, ALL, or one of the group options (*groupopt*), all of which include SSCP as an individual option equivalent. The group options are APIOPTS, APPCOPTS, CPCPOPTS, CSMOPTS, DLUROPTS, EEOPTS, HPDTOPTS, HPROPTS, LCSOPTS, QDIOOPTS, STDOPTS, TCPOPTS, and XCFOPTS.

16 If multiple trace options are coded in parentheses, either SSCP or one of the group options (*groupopt*) must be coded inside the parentheses when SUBTRACE=TGVC or SUBTRACE=TREE is coded.

AIMON start option

Determines whether VTAM monitors interfaces for overdue adapter interrupts. If an overdue adapter interrupt is detected, VTAM will drive a virtual interrupt in an effort to prevent a stall condition.VTAM will also issue message IST2419I when an overdue interrupt is detected.

Guideline: Specify NONE unless requested by IBM service.

AIMON=NONE
Specifies that VTAM does not monitor adapter interrupts for any interfaces.

AIMON=ISM
Specifies that VTAM monitors adapter interrupts for internal shared memory (ISM) interfaces.

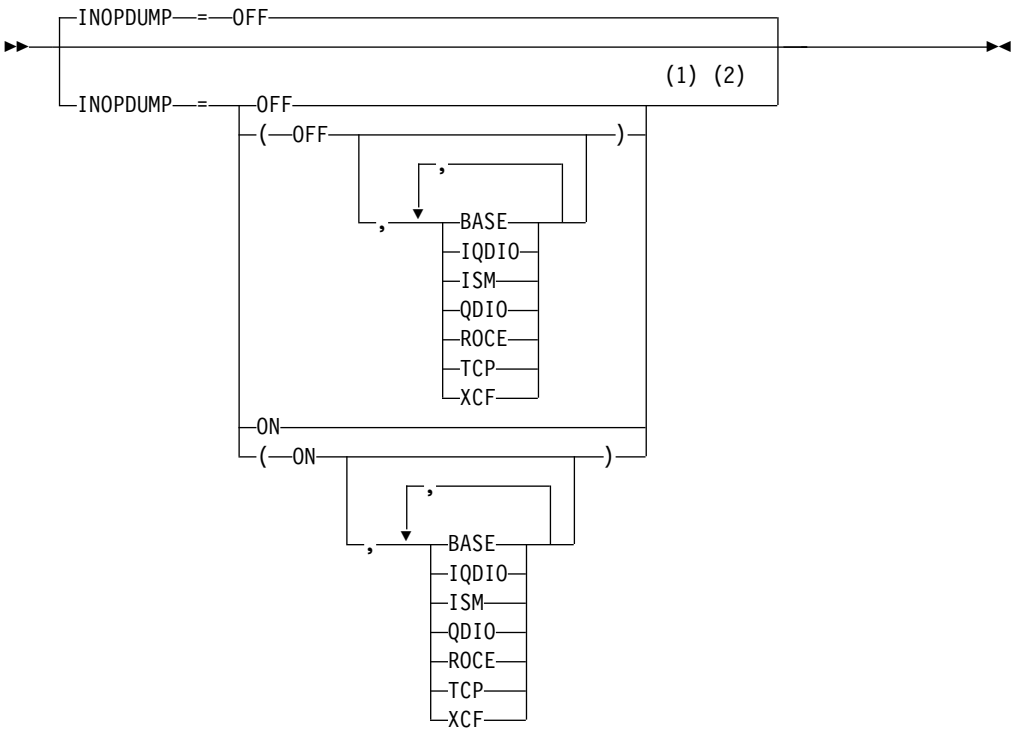
AIMON=QDIO
Specifies that VTAM monitors adapter interrupts for OSA-Express interfaces. CHPID types include OSD, OSM and OSX.

AIMON=ROCE
Specifies that VTAM monitors adapter interrupts for 10GbE RoCE Express interfaces.

Usage: You can specify only one adapter for an individual AIMON start option instance. However, if you code multiple AIMON start options, the results are cumulative. For example, to start interface monitoring for 10GbE RoCE Express and ISM interfaces, you can code the following start option values:

```
AIMON=ROCE
AIMON=ISM
```

INOPDUMP start option



Notes:

1 INOPDUMP status is propagated to resources that are defined within a transport resource list entry when the entry is activated.

2 The INOPCODE start option provides more granular control of the

INOPDUMP function. Refer to the INOPCODE in this section and the DISPLAY INOPCODE command in z/OS Communications Server: SNA Operation for additional details.

Specifies whether VTAM dumps should be generated whenever VTAM detects certain inoperative conditions.

INOPDUMP is used to enable and disable diagnostic dumps for certain channel related inoperative conditions. INOPDUMP can be set in the following manner:

- Globally set for all channel related resources.
- Selectively set for a subset of resources that INOPDUMP control groups identify.
- Individually set for a specific TRLE by the MODIFY INOPDUMP command.

INOPCODE is used to enable and disable dumping for a specific INOPCODE. See INOPCODE start option and z/OS Communications Server: SNA Operation for additional details about how these functions interact.

You can change the INOPDUMP value with the MODIFY VTAMOPTS command while VTAM is running. You can also change the INOPDUMP value or apply a value to a specific TRLE or set of TRLEs with the MODIFY INOPDUMP command while VTAM is running.

Global INOPDUMP settings

INOPDUMP=OFF
Specifies that dumps are not taken.

INOPDUMP=ON
Specifies that dumps are taken.

Selective INOPDUMP settings by control groups

INOPDUMP=(OFF,*ctlgrp***,***ctrlgrp***,..***ctrlgrp***)**
Specifies that dumps are not taken for resources that are associated with the identified control groups.

INOPDUMP=(ON,*ctlgrp***,***ctrlgrp***,..***ctrlgrp***)**
Specifies that dumps are taken for resources that are associated with the identified control groups.

The INOPDUMP control group *ctrlgrp* can be one of the following values:

BASE Includes the IUTSAMEH and AHHC TRLE control resources, as well as all non-TRLE based channel resources. For example, Local SNA (PU4/PU2), CTC, MPC, and LCS.

IQDIO
Includes all TRLEs that are associated with Hipersockets.

ISM Includes all TRLEs that are associated with Shared Memory Communications - Direct Memory Access (SMC-D).

QDIO Includes all TRLEs that are associated with OSA-Express adapters. CHPID types include OSD, OSM and OSX.

ROCE Includes all TRLEs that are associated with Shared Memory Communications over RDMA enhancements (SMC-R).

TCP Includes all TRLEs that are associated with TCP exclusive DLCs. For example, CTC and LCS.

XCF Includes all TRLEs that are associated with XCF sysplex connections.

Chapter 13. Quick Reference

Display workload information for a device

Storage problems can be related to a specific I/O device. Because outbound data cannot be transmitted to an I/O device until it is accepted by that device (that is, until write processing completes), there are scenarios in which this storage associated with this data can accumulate at the DLC (data link control) layer. For all I/O devices that perform real I/O that are represented by a TRLE (predefined or dynamically built), VTAM tracks the outbound workload (units of work) for each device. This tracking mechanism allows console operators to isolate this type of problem to a specific device.

The console operator can quickly isolate a storage problem to a specific device using the DISPLAY TRL command. If a device has exceeded internal thresholds, message IST1800I is issued with the text `** CONGESTED **`. Additional details regarding the workload for a specific device are displayed with the DISPLAY TRL,TRLE=*trlename* command. VTAM displays the current, average, and the maximum workload for each device. When the current workload is excessive, the I/O activity for this device might be associated with system storage shortages.

If the counts for a device reveal an excessive current workload, additional steps are required to isolate the problem.

- **Steps for a console operator**

  When a device is marked as congested, further action is required to determine whether the congestion is related to a system storage problem. If the following steps indicate that a system storage shortage is present, it might be necessary to obtain documentation (such as a console log and a dump) to diagnose the congestion related to this device. This condition might be relieved by deactivating the PU (or stopping the device for TCP/IP).

  1. Review the system console for any messages related to current storage shortage conditions.
  2. Issue the following VTAM display commands:
     - D NET,CSM
     - D NET,BFRUSE
     - D NET,STORUSE,POOL=*

     Note: If applicable, also issue the TCP/IP DISPLAY command D TCPIP,,STOR.
  3. Issue D NET,TRL,TRLE=*trlename* to obtain more details about the device congestion. Message IST1802I displays detailed counts of units of work for the device measured at the Data Link Control (DLC) layer.
  4. Activate VTAM tuning statistics (TNSTAT), RMF™, or other monitoring tools to monitor this specific device.
  5. Display the active jobs in the system to determine whether new work was recently started.

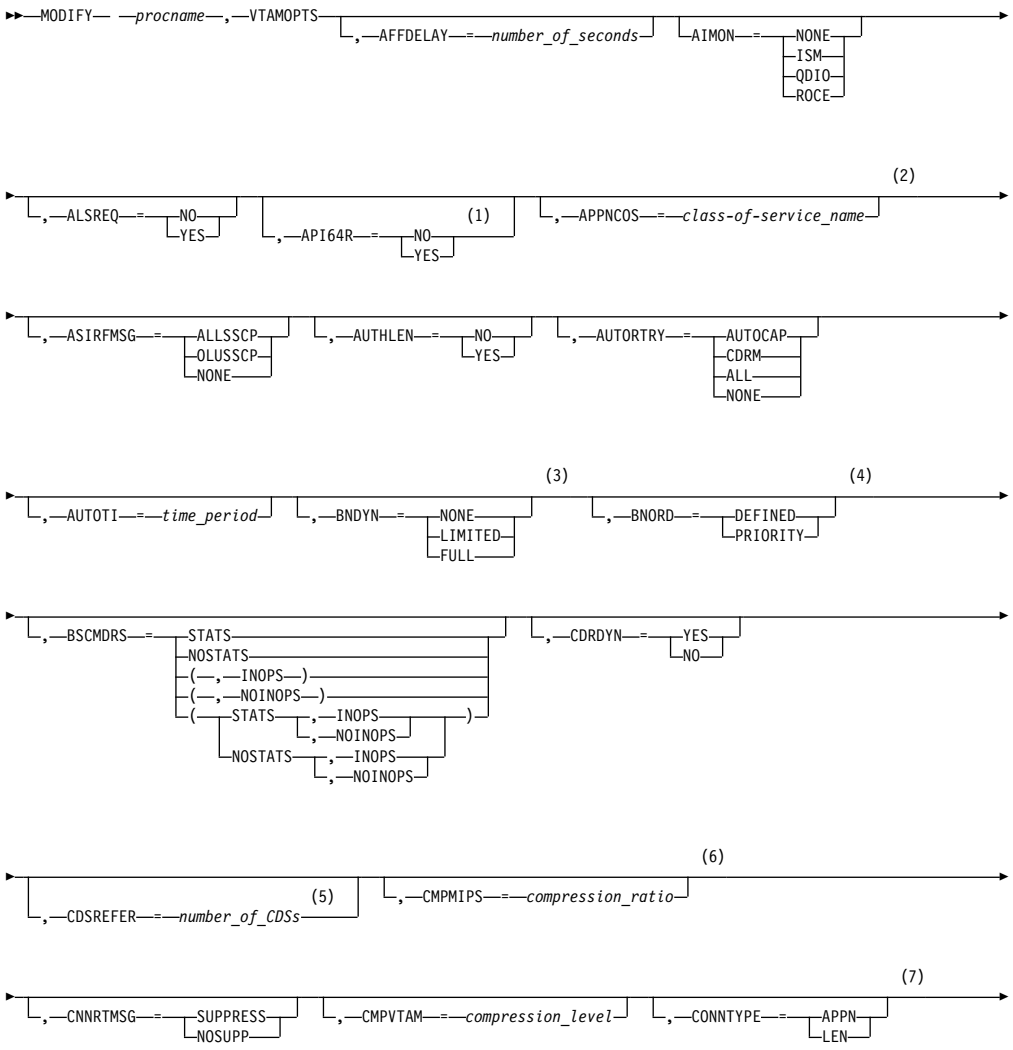
- **Steps for a system programmer**

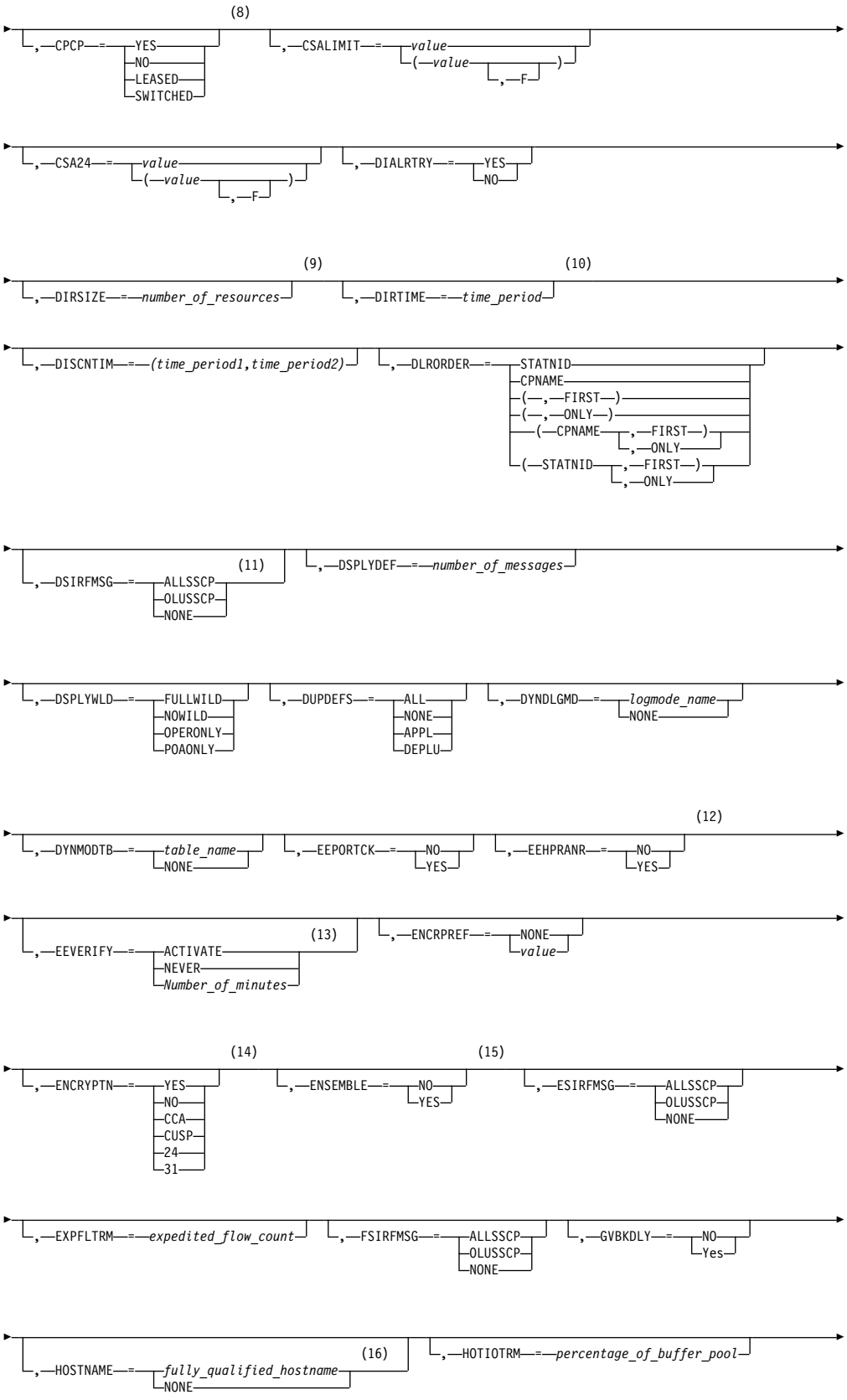
  The following steps might be required to isolate a system storage problem that is related to an I/O device:

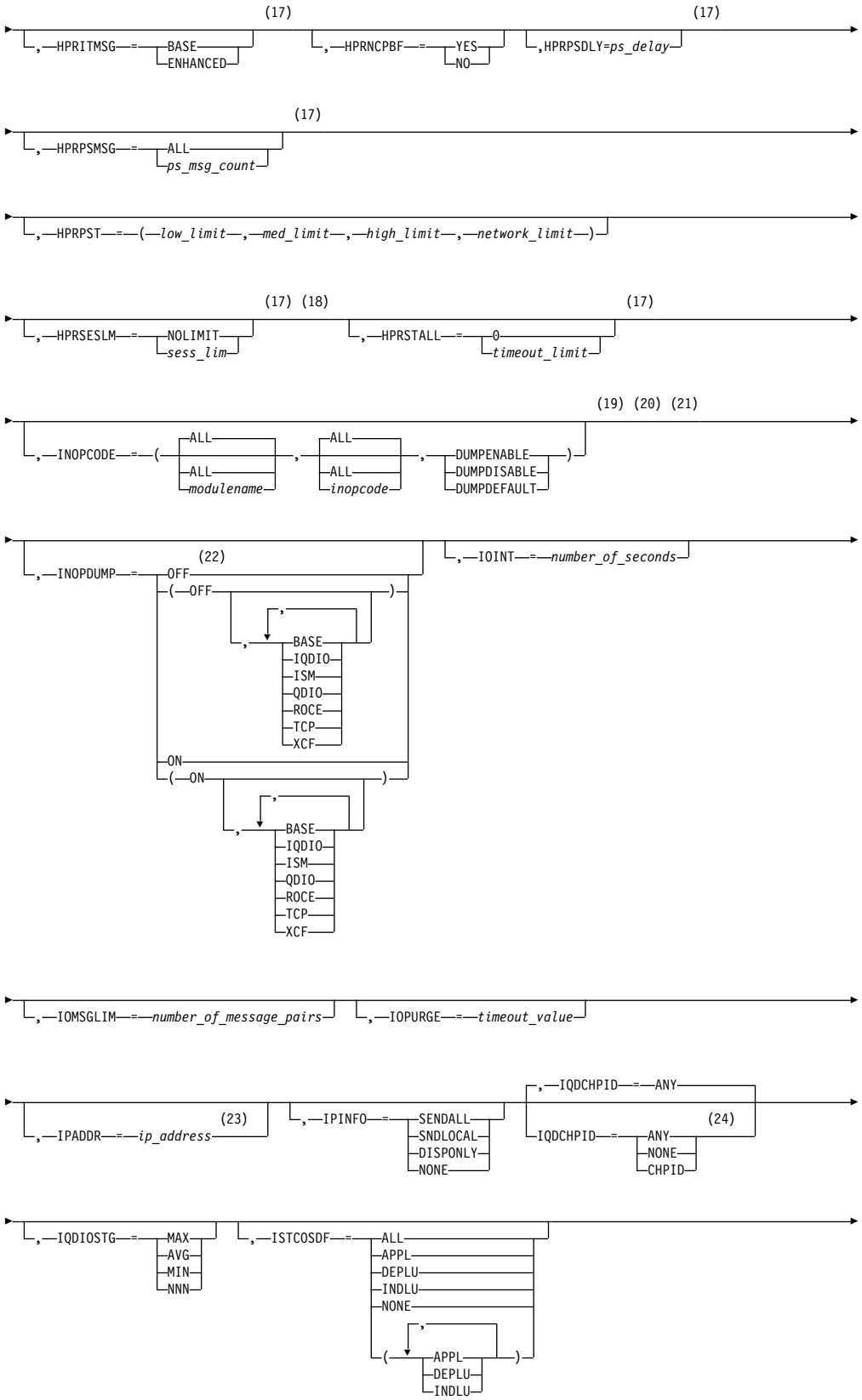
1. Review the network configuration related to this device or any recent configuration changes for this system.
2. Review or monitor (using the output from VTAM TNSTAT or RMF) the network traffic related to this device. Compare the actual workload to the I/O capacity of the hardware device.
3. Determine if the congestion is related to a specific time of day, job, application, or type of workload.
4. Verify that missing interrupt handler (MIH) is enabled for the write devices.
5. Review or verify that the maintenance level for the hardware device is current.
6. Consider automating the necessary storage displays to monitor system conditions.

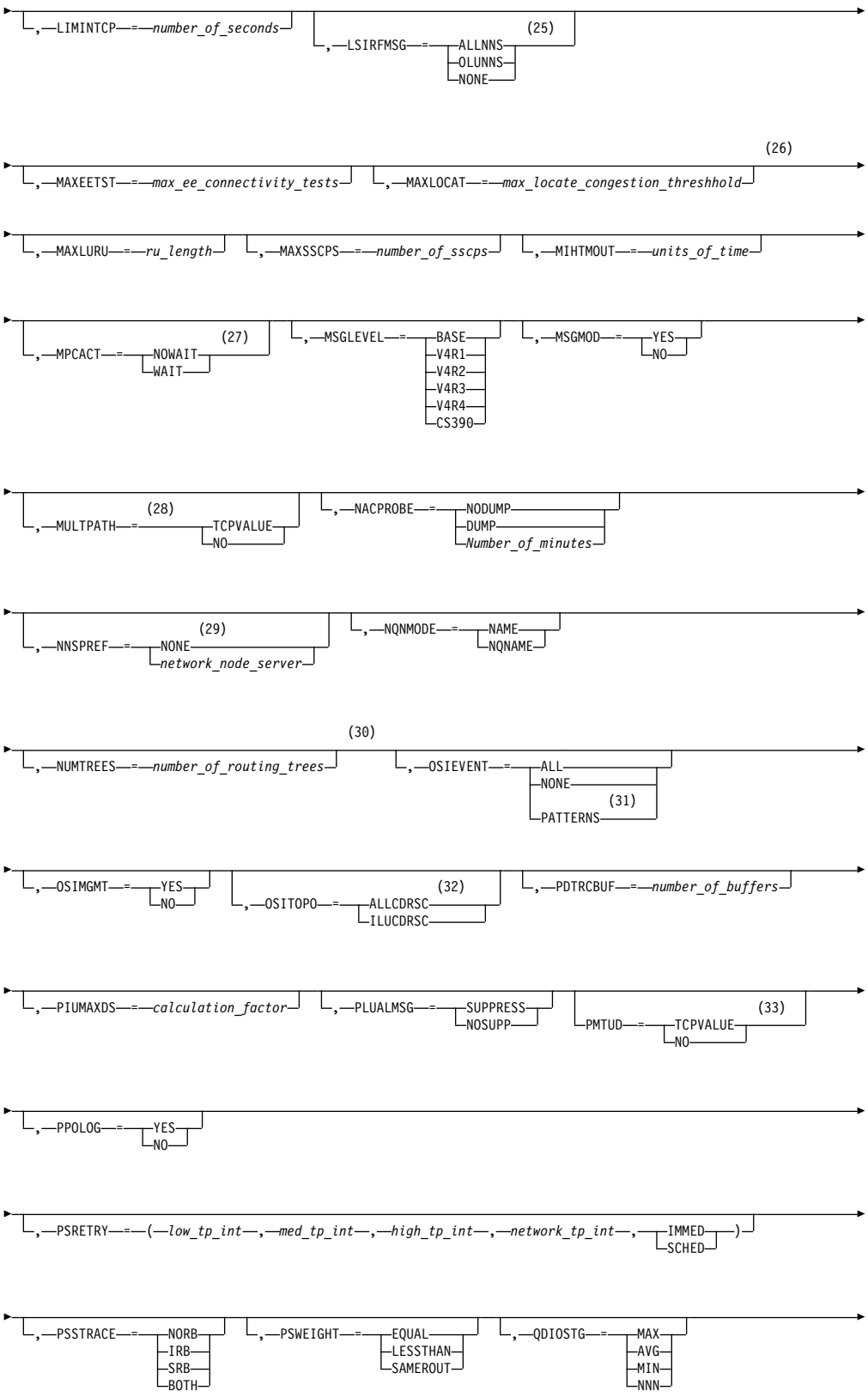
F VTAMOPTS command

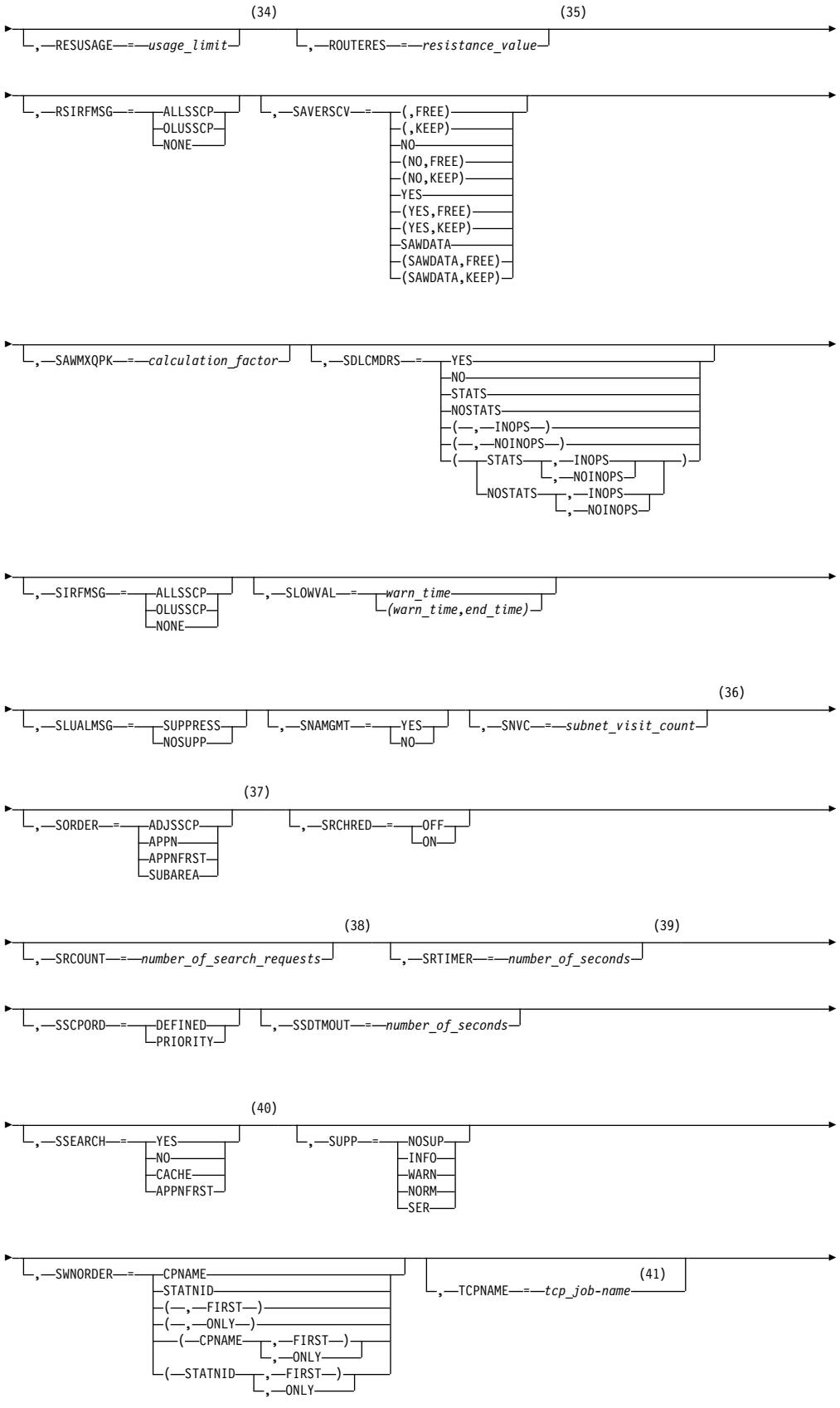
Change certain values that might have been specified on VTAM start options:

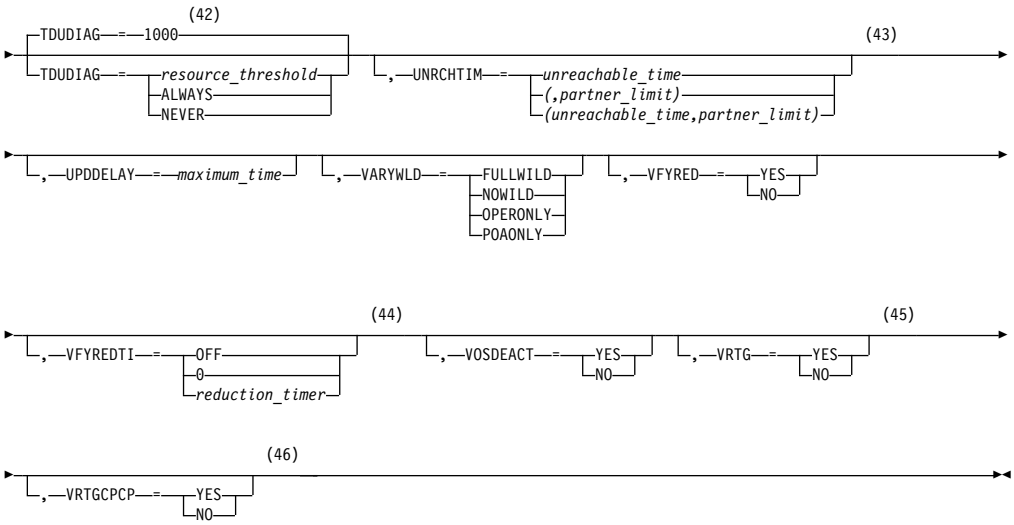



(8)
,—CPCP—=—YES
NO
LEASED
SWITCHED
,—CSALIMIT—=—value
(—value—,—F—)
,—CSA24—=—value
(—value—,—F—)
,—DIALRTRY—=—YES
NO
(9)
,—DIRSIZE—=—number_of_resources
(10)
,—DIRTIME—=—time_period
,—DISCNTIM—=—(time_period1,time_period2)
,—DLRORDER—=—STATNID
CPNAME
(—,—FIRST—)
(—,—ONLY—)
(—CPNAME—,—FIRST—)
,—ONLY
(—STATNID—,—FIRST—)
,—ONLY
(11)
,—DSIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—DSPLYDEF—=—number_of_messages
,—DSPLYWLD—=—FULLWILD
NOWILD
OPERONLY
POAONLY
,—DUPDEFS—=—ALL
NONE
APPL
DEPLU
,—DYNDLGMD—=—logmode_name
NONE
(12)
,—DYNMODTB—=—table_name
NONE
,—EEPORTCK—=—NO
YES
,—EEHPRANR—=—NO
YES
(13)
,—EEVERIFY—=—ACTIVATE
NEVER
Number_of_minutes
,—ENCRPREF—=—NONE
value
(14)
,—ENCRYPTN—=—YES
NO
CCA
CUSP
24
31
(15)
,—ENSEMBLE—=—NO
YES
,—ESIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—EXPFLTRM—=—expedited_flow_count
,—FSIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—GVBKDLY—=—NO
Yes
(16)
,—HOSTNAME—=—fully_qualified_hostname
NONE
,—HOTIOTRM—=—percentage_of_buffer_pool


(17)
,HPRITMSG=BASE
ENHANCED
,HPRNCPBF=YES
NO
(17)
,HPRPSDLY=ps_delay
(17)
,HPRPSMSG=ALL
ps_msg_count
,HPRPST=(low_limit,med_limit,high_limit,network_limit)
(17) (18)
,HPRSESLM=NOLIMIT
sess_lim
(17)
,HPRSTALL=0
timeout_limit
(19) (20) (21)
,INOPCODE=(ALL
ALL
modulename,ALL
ALL
inopcode,DUMPENABLE
DUMPDISABLE
DUMPDEFAULT)
(22)
,INOPDUMP=OFF
(OFF)
BASE
IQDIO
ISM
QDIO
ROCE
TCP
XCF
ON
(ON)
BASE
IQDIO
ISM
QDIO
ROCE
TCP
XCF
,IOINT=number_of_seconds
,IOMSGLIM=number_of_message_pairs
,IOPURGE=timeout_value
(23)
,IPADDR=ip_address
,IPINFO=SENDALL
SNDLOCAL
DISPONLY
NONE
,IQDCHPID=ANY
(24)
IQDCHPID=ANY
NONE
CHPID
,IQDIOSTG=MAX
AVG
MIN
NNN
,ISTCOSDF=ALL
APPL
DEPLU
INDLU
NONE
(APPL
DEPLU
INDLU)


,LIMINTCP=number_of_seconds
,LSIRFMSG=(25) ALLNNS OLUNNS NONE
,MAXEETST=max_ee_connectivity_tests
,MAXLOCAT=max_locate_congestion_threshhold (26)
,MAXLURU=ru_length
,MAXSSCPS=number_of_sscps
,MIHTMOUT=units_of_time
,MPCACT=(27) NOWAIT WAIT
,MSGLEVEL=BASE V4R1 V4R2 V4R3 V4R4 CS390
,MSGMOD=YES NO
,MULTPATH=(28) TCPVALUE NO
,NACPROBE=NODUMP DUMP Number_of_minutes
,NNSPREF=(29) NONE network_node_server
,NQNMODE=NAME NQNAME
,NUMTREES=number_of_routing_trees (30)
,OSIEVENT=ALL NONE PATTERNS (31)
,OSIMGMT=YES NO
,OSITOPO=(32) ALLCDRSC ILUCDRSC
,PDTRCBUF=number_of_buffers
,PIUMAXDS=calculation_factor
,PLUALMSG=SUPPRESS NOSUPP
PMTUD=(33) TCPVALUE NO
,PPOLOG=YES NO
,PSRETRY=(low_tp_int,med_tp_int,high_tp_int,network_tp_int,IMMED SCHED)
,PSSTRACE=NORB IRB SRB BOTH
,PSWEIGHT=EQUAL LESSTHAN SAMEROUT
,QDIOSTG=MAX AVG MIN NNN


(34)
(35)
,—RESUSAGE—=—usage_limit
,—ROUTERES—=—resistance_value
,—RSIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—SAVERSCV—=—(,FREE)
(,KEEP)
NO
(NO,FREE)
(NO,KEEP)
YES
(YES,FREE)
(YES,KEEP)
SAWDATA
(SAWDATA,FREE)
(SAWDATA,KEEP)
,—SAWMXQPK—=—calculation_factor
,—SDLCMDRS—=—YES
NO
STATS
NOSTATS
(—,—INOPS—)
(—,—NOINOPS—)
(—STATS—,—INOPS
,—NOINOPS
)
NOSTATS—,—INOPS
,—NOINOPS
,—SIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—SLOWVAL—=—warn_time
(warn_time,end_time)
(36)
,—SLUALMSG—=—SUPPRESS
NOSUPP
,—SNAMGMT—=—YES
NO
,—SNVC—=—subnet_visit_count
(37)
,—SORDER—=—ADJSSCP
APPN
APPNFRST
SUBAREA
,—SRCHRED—=—OFF
ON
(38)
(39)
,—SRCOUNT—=—number_of_search_requests
,—SRTIMER—=—number_of_seconds
,—SSCPORD—=—DEFINED
PRIORITY
,—SSDTMOUT—=—number_of_seconds
(40)
,—SSEARCH—=—YES
NO
CACHE
APPNFRST
,—SUPP—=—NOSUP
INFO
WARN
NORM
SER
,—SWNORDER—=—CPNAME
STATNID
(—,—FIRST—)
(—,—ONLY—)
(—CPNAME—,—FIRST—)
,—ONLY
(—STATNID—,—FIRST—)
,—ONLY
(41)
,—TCPNAME—=—tcp_job-name



Notes:

1 API64R can be modified only when running in z/Architecture mode.

2 APPNCOS can be modified only if NODETYPE was specified during VTAM START processing.

3 BNDYN can be modified only if BN=YES was specified during VTAM START processing.

4 BNORD can be modified only if BN=YES was specified during VTAM START processing.

5 CDSREFER can be modified only if NODETYPE=NN and CDSERVR=NO were specified during VTAM START processing.

6 CMPMIPS is meaningful only if the value for CMPVTAM is greater than 1.

7 CONNTYPE can be modified only if NODETYPE was specified during VTAM START processing.

8 CPCP can be modified only if NODETYPE was specified during VTAM START processing.

9 DIRSIZE can be modified only if NODETYPE=NN was specified during VTAM START processing.

10 DIRTIME can be modified only if NODETYPE=NN was specified during VTAM START processing.

11 Because of the volume of messages that can be generated, it is not recommended that this option be enabled during normal operation. Instead, it is recommended that this option be enabled (using the MODIFY VTAMOPTS command) on all necessary hosts only when trying to diagnose specific problems. After the problem has been diagnosed or documentation has been collected, this option should be disabled once again (using the MODIFY VTAMOPTS command).

12 EEHPRANR is meaningful only when the NODETYPE=NN start option is also used.

13 The EEVERIFY start option is meaningful only if VTAM provides RTP-level

HPR support. The EEVERIFY start option can be modified only if the NODETYPE start option is specified and the RTP value is specified on the HPR start option.

14 The ENCRYPTN start option cannot be modified if ENCRYPTN=NO was specified during VTAM START processing.

15 The ENSEMBLE setting is used to either permit or deny connectivity to the intraensemble data network and the intranode management network. The ensemble setting permits or denies connectivity by either allowing or denying activation of OSX and OSM interfaces. Modifying the ENSEMBLE start option does not cause z/OS Communications Server to take action on active OSX or OSM interfaces.

16 HOSTNAME can be modified only if NODETYPE was specified during VTAM START processing. Displays of VTAM start options will show the new value immediately; however, the new value will not be used until all Enterprise Extender lines, whose GROUP definition statements do not have HOSTNAME explicitly coded, are inactive. Any subsequent line activation from the Enterprise Extender XCA major node, whose GROUP definition statements do not have HOSTNAME explicitly coded, will make use of the new HOSTNAME start option value. The IPADDR start option, if it is in effect at the time when the MODIFY VTAMOPTS,HOSTNAME=*hostname* is specified, will be reset (that is, set to a value of 0.0.0.0) as part of the MODIFY processing. The value NONE can be used to clear the setting of the HOSTNAME start option. HOSTNAME and IPADDR cannot be modified using one MODIFY VTAMOPTS command. If both start options are specified on the same MODIFY command, they will both be ignored and message IST1917I will be generated.

17 This option is meaningful only if VTAM provides RTP-level HPR support.

18 If the current value of the HPRSESLM start option is DISABLED, then the HPRSESLM value can be changed only by stopping and restarting VTAM.

19 When specifying an InOpCode for the second parameter, always specify three digits by including any leading zeros.

20 If an InOpCode is specified for the second parameter, the first parameter cannot be ALL.

21 INOPCODE has no effect unless INOPDUMP is active for the resource when an inoperative condition is detected. See the section called MODIFY INOPCODE command for more details.

22 When altering the INOPDUMP VTAM start option, the resulting INOPDUMP status is propagated to all TRLEs in the TRL major node if the command is globally set, or it is propogated to a subset of resources that are identified by one or more INOPDUMP control groups. The INOPDUMP setting becomes the default status for any subsequently activated TRLEs.

23 IPADDR can be modified only if NODETYPE was specified during VTAM START processing. The new value will not be used until all lines, defined with or defaulting to the old value of the IPADDR start option, in the XCA major node used for Enterprise Extender are inactive. However, displays of VTAM start options will show the new value immediately. Any subsequent line activation from the Enterprise Extender XCA major node, whose GROUP definition statement does not specify the IPADDR operand, will make use of the new IPADDR start option value. The HOSTNAME start option, if it is in effect at the time when the MODIFY VTAMOPTS,IPADDR=*ip_address* is specified, will be reset (that is, set to a value of NONE) as part of the

MODIFY processing. The value of 0.0.0.0, or an IPv6 address of all zeros, usually written as ::, can be used to clear the setting of the IPADDR start option. HOSTNAME and IPADDR cannot be modified using one MODIFY VTAMOPTS command. If both start options are specified on the same MODIFY command, they will both be ignored and message IST1917I will be generated.

24 The IQDCHPID option controls which IQD CHPID (and related subchannel devices) VTAM selects to dynamically build the iQDIO (IUTIQDIO) MPC group. The IUTIQDIO MPC group is used for TCP/IP dynamic XCF communications within System z. Although this option can be modified (and the modification will immediately be displayed) while the IUTIQDIO MPC group is currently active, any modifications have the effects shown in the section called IQD CHPID modifications.

25 Because of the volume of messages that can be generated, it is not recommended that this option be enabled during normal operation. Instead, it is recommended that this option be enabled (using the MODIFY VTAMOPTS command) on all necessary hosts only when trying to diagnose specific problems. After the problem has been diagnosed or documentation has been collected, this option should be disabled once again (using the MODIFY VTAMOPTS command).

26 MAXLOCAT can be modified only if NODETYPE was specified during VTAM START processing.

27 The option does not take effect for MPC groups that are in the process of being activated when the command is issued until those MPC groups are deactivated and reactivated.

28 MULTPATH is meaningful only if the NODETYPE start option is also specified.

29 NNSPREF can be modified only if NODETYPE=EN was specified during VTAM START processing.

30 NUMTREES can be modified only if NODETYPE=NN was specified during VTAM START processing.

31 OSIEVENT=PATTERNS is not valid when OSIMGMT=YES.

32 OSITOPO=ALLCDRSC is not valid when OSIMGMT=YES.

33 PMTUD is meaningful only if the NODETYPE start option is also specified.

34 RESUSAGE can be modified only if NODETYPE=NN was specified during VTAM START processing.

35 ROUTERES can be modified only if NODETYPE=NN was specified during VTAM START processing.

36 SNVC can be modified only if BN=YES was specified during VTAM START processing.

37 SORDER can be modified only if VTAM has been started as an interchange node or a migration data host.

38 SRCOUNT is meaningful only when SRCHRED=ON.

39 SRTIMER is meaningful only when SRCHRED=ON.

40 SSEARCH can be modified only if NODETYPE=NN was specified during VTAM START processing.

41 TCPNAME can be modified only if NODETYPE was specified during VTAM

START processing. The new value will not be used until all lines in the XCA major node used for Enterprise Extender are inactive. However, displays of VTAM start options will show the new value immediately. Any subsequent line activation from the Enterprise Extender XCA major node will make use of the new TCPNAME value.

42 TDUDIAG is meaningful only if the NODETYPE=NN start option is also available.

43 UNRCHTIM is meaningful only if the NODETYPE start option is also used.

44 VFYREDTI can be modified only if NODETYPE=NN was specified during VTAM START processing.

45 VRTG can be modified only if NODETYPE and HOSTSA are specified.

46 VRTGCPCP can be modified only if NODETYPE and HOSTSA are specified.

Start options

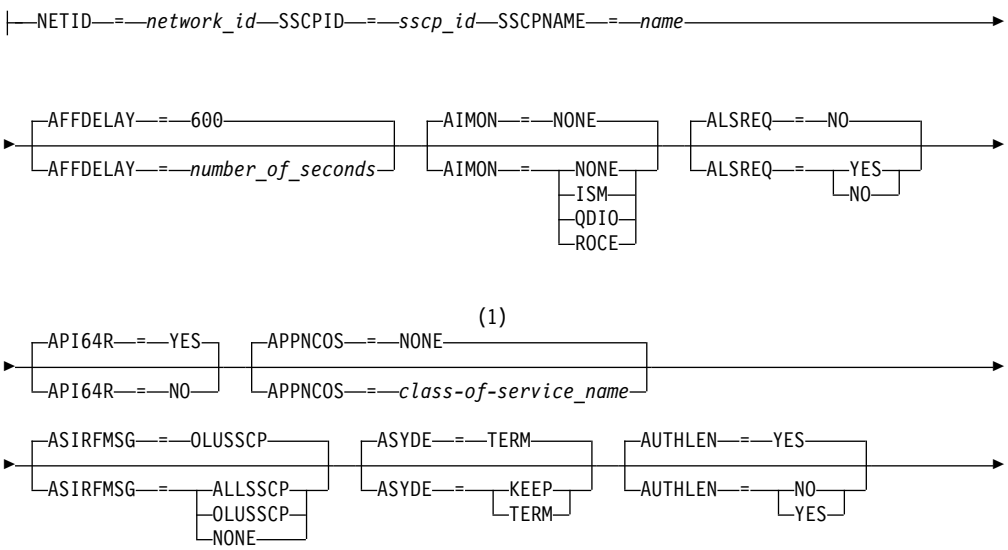
Start options are listed in this section alphabetically; however, you can code them in any order.

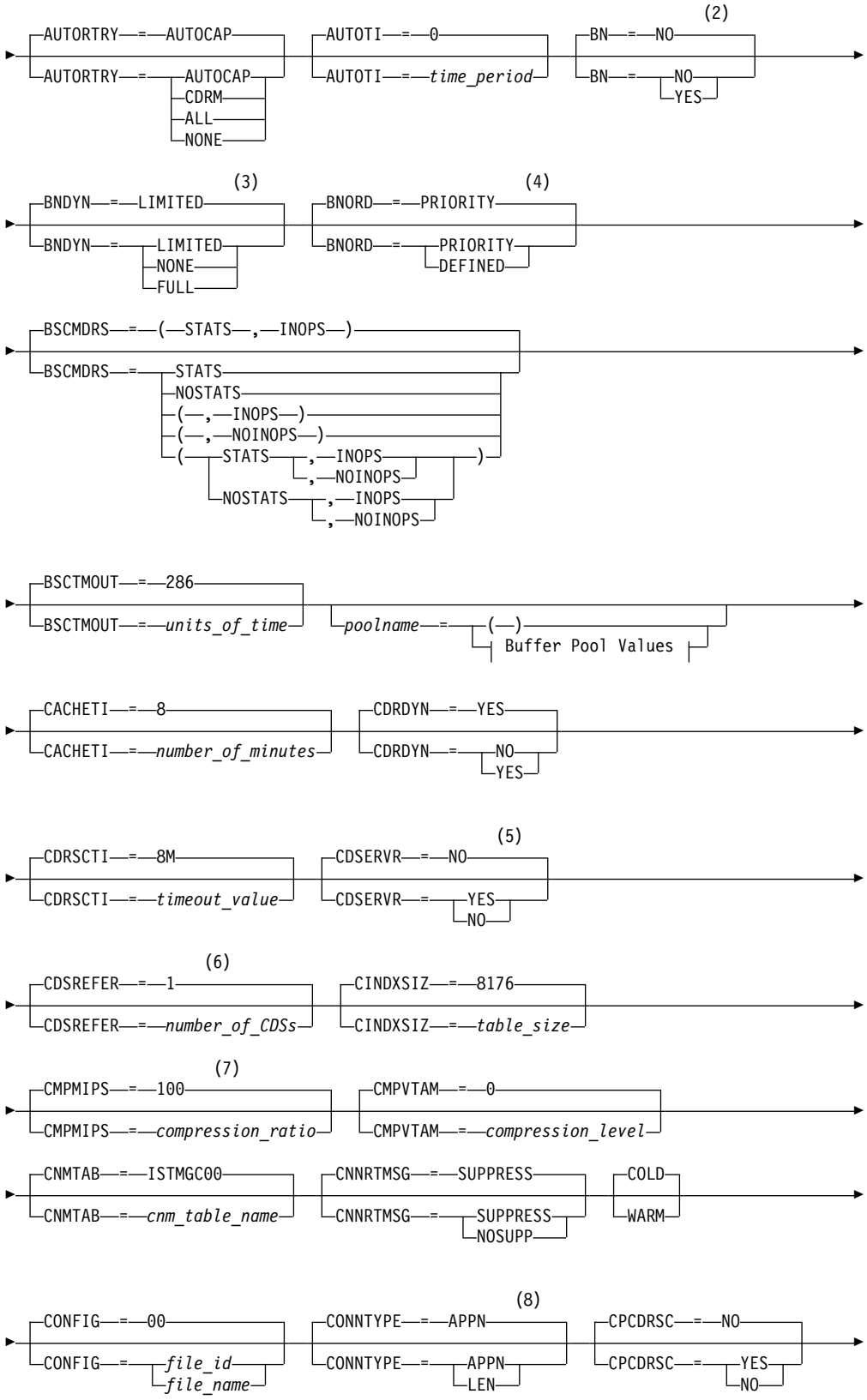
Precede the option list with three commas and enclose the group of options in parentheses.

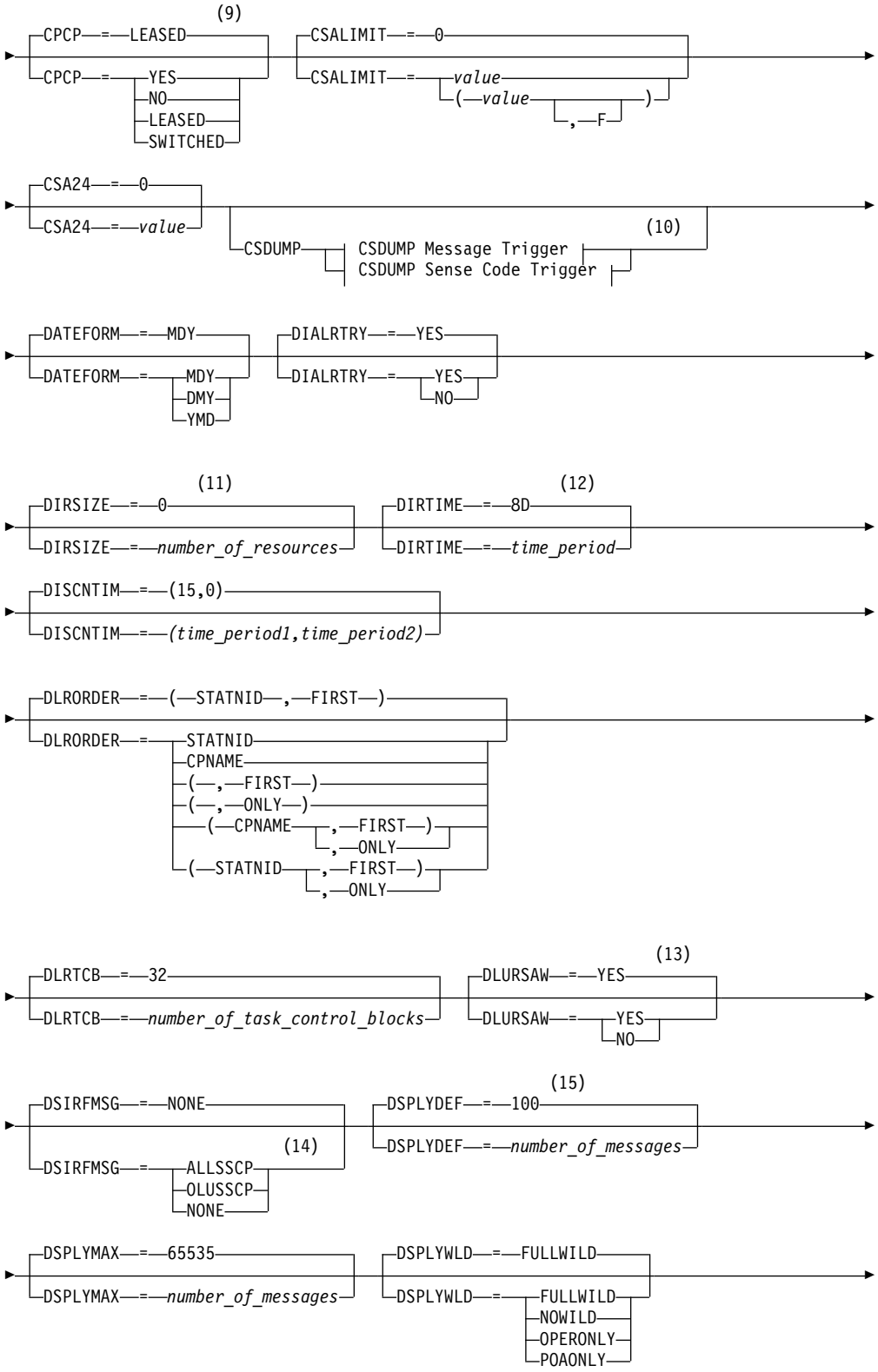
Start options that are entered on the START command must be separated by commas. Do not leave any blanks between options.

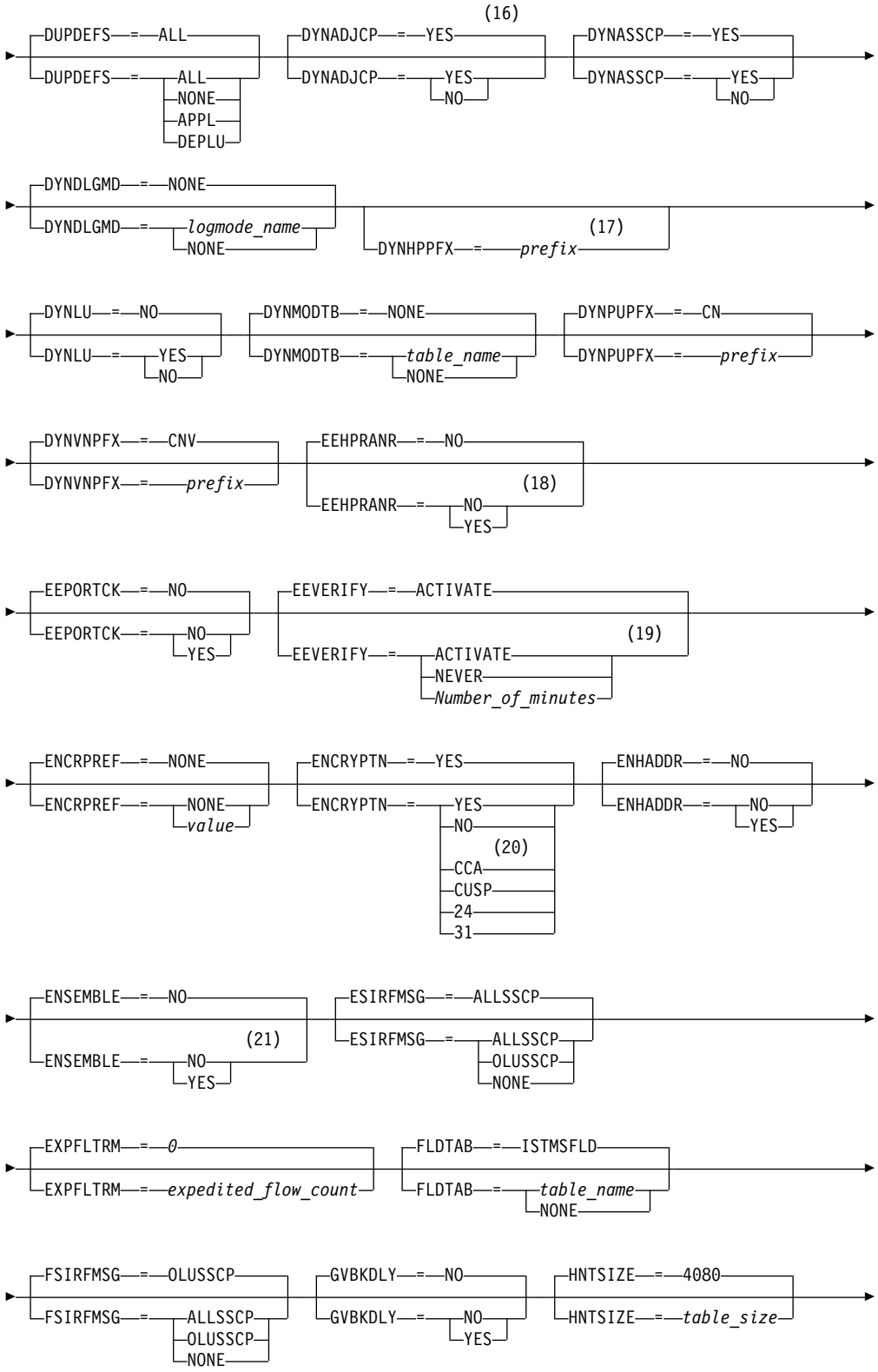
For more information on the START command, see z/OS Communications Server: SNA Operation.

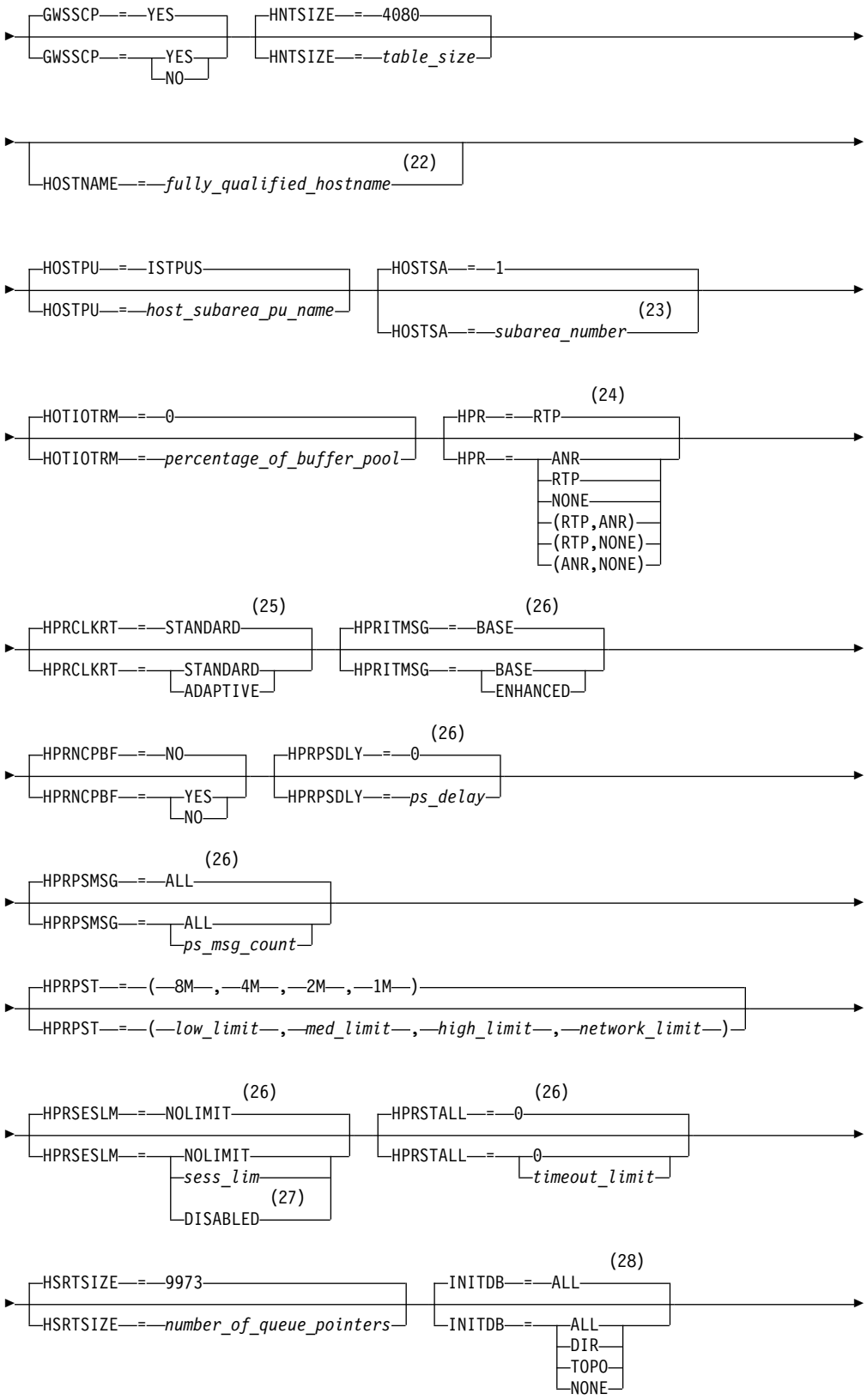
Options:

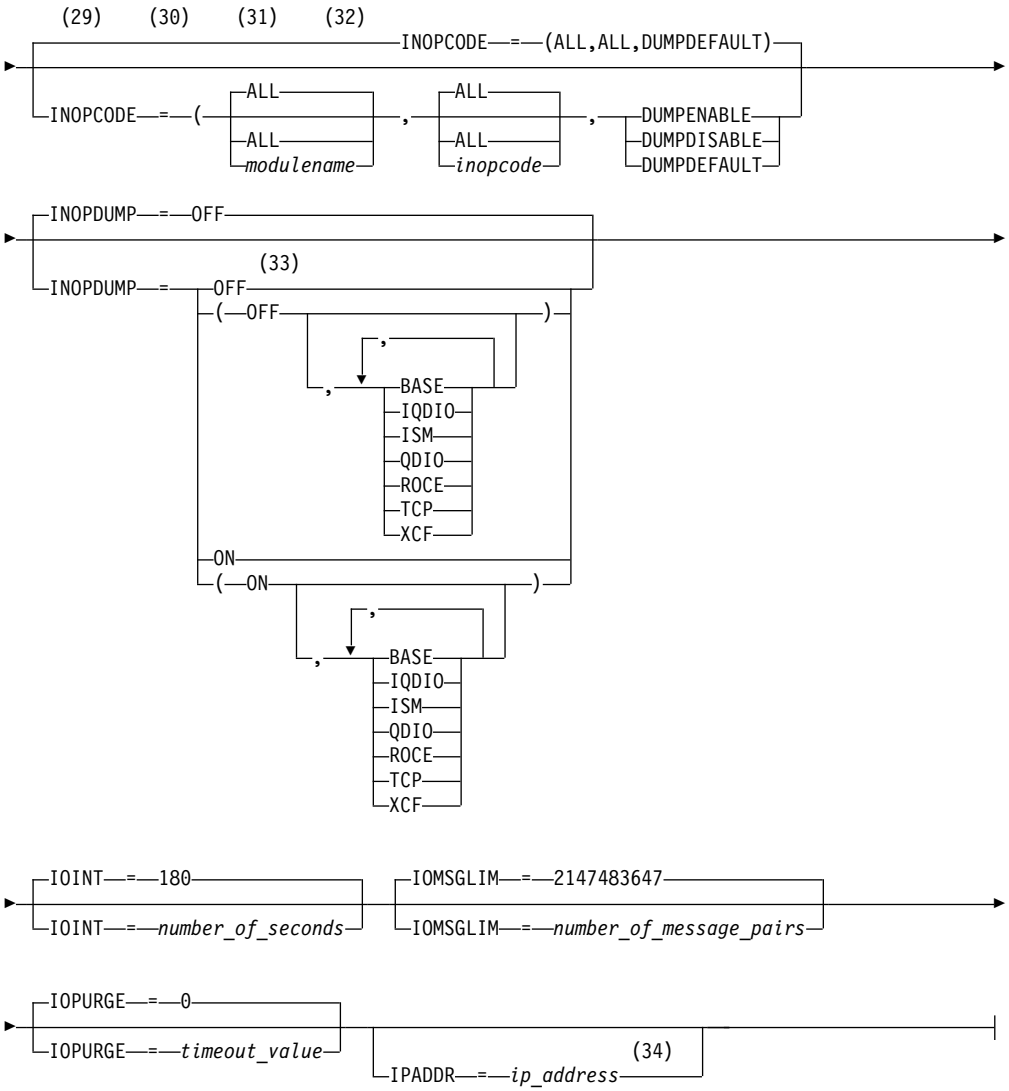



AUTORTRY
AUTOCAP
CDRM
ALL
NONE
AUTOTI
0
time_period
(2)
BN
NO
YES
BNDYN
LIMITED
NONE
FULL
(3)
BNORD
PRIORITY
DEFINED
(4)
BSCMDRS
STATS
INOPS
NOINOPS
NOSTATS
BSCTMOUT
286
units_of_time
poolname
Buffer Pool Values
CACHETI
8
number_of_minutes
CDRDYN
YES
NO
CDRSCTI
8M
timeout_value
CDSERVR
(5)
CDSREFER
1
number_of_CDSs
(6)
CINDXSIZ
8176
table_size
CMPMIPS
100
compression_ratio
(7)
CMPVTAM
0
compression_level
CNMTAB
ISTMGC00
cnm_table_name
CNNRTMSG
SUPPRESS
NOSUPP
COLD
WARM
CONFIG
00
file_id
file_name
CONNTYPE
APPN
LEN
(8)
CPCDRSC
YES
NO


(9)
CPCP=LEASED
CPCP=YES
NO
LEASED
SWITCHED
CSALIMIT=0
CSALIMIT=value
(value)
,F
CSA24=0
CSA24=value
(10)
CSDUMP
CSDUMP Message Trigger
CSDUMP Sense Code Trigger
DATEFORM=MDY
DATEFORM=MDY
DMY
YMD
DIALRTRY=YES
DIALRTRY=YES
NO
(11)
DIRSIZE=0
DIRSIZE=number_of_resources
(12)
DIRTIME=8D
DIRTIME=time_period
DISCNTIM=(15,0)
DISCNTIM=(time_period1,time_period2)
DLRORDER=(STATNID,FIRST)
DLRORDER=
STATNID
CPNAME
(,FIRST)
(,ONLY)
(CPNAME
,FIRST)
,ONLY
(STATNID
,FIRST)
,ONLY
DLRTCB=32
DLRTCB=number_of_task_control_blocks
(13)
DLURSAW=YES
DLURSAW=
YES
NO
DSIRFMSG=NONE
(14)
DSIRFMSG=
ALLSSCP
OLUSSCP
NONE
(15)
DSPLYDEF=100
DSPLYDEF=number_of_messages
DSPLYMAX=65535
DSPLYMAX=number_of_messages
DSPLYWLD=FULLWILD
DSPLYWLD=
FULLWILD
NOWILD
OPERONLY
POAONLY


(16)
DUPDEFS
ALL
DUPDEFS
ALL
NONE
APPL
DEPLU
DYNADJCP
YES
DYNADJCP
YES
NO
DYNASSCP
YES
DYNASSCP
YES
NO
DYNDLGMD
NONE
DYNDLGMD
logmode_name
NONE
(17)
DYNHPPFX
prefix
DYNLU
NO
DYNLU
YES
NO
DYNMODTB
NONE
DYNMODTB
table_name
NONE
DYNPUPFX
CN
DYNPUPFX
prefix
DYNVNPFX
CNV
DYNVNPFX
prefix
EEHPRANR
NO
(18)
EEHPRANR
NO
YES
EEPORTCK
NO
EEPORTCK
NO
YES
EEVERIFY
ACTIVATE
(19)
EEVERIFY
ACTIVATE
NEVER
Number_of_minutes
ENCRPREF
NONE
ENCRPREF
NONE
value
ENCRYPTN
YES
ENCRYPTN
YES
NO
(20)
CCA
CUSP
24
31
ENHADDR
NO
ENHADDR
NO
YES
ENSEMBLE
NO
(21)
ENSEMBLE
NO
YES
ESIRFMSG
ALLSSCP
ESIRFMSG
ALLSSCP
OLUSSCP
NONE
EXPFLTRM
0
EXPFLTRM
expedited_flow_count
FLDTAB
ISTMSFLD
FLDTAB
table_name
NONE
FSIRFMSG
OLUSSCP
FSIRFMSG
ALLSSCP
OLUSSCP
NONE
GVBKDLY
NO
GVBKDLY
NO
YES
HNTSIZE
4080
HNTSIZE
table_size


GWSSCP
=
YES
NO
HNTSIZE
4080
table_size
HOSTNAME
fully_qualified_hostname
(22)
HOSTPU
ISTPUS
host_subarea_pu_name
HOSTSA
1
subarea_number
(23)
HOTIOTRM
0
percentage_of_buffer_pool
HPR
RTP
ANR
NONE
(RTP,ANR)
(RTP,NONE)
(ANR,NONE)
(24)
HPRCLKRT
STANDARD
ADAPTIVE
(25)
HPRITMSG
BASE
ENHANCED
(26)
HPRNCPBF
NO
YES
HPRPSDLY
0
ps_delay
HPRPSMSG
ALL
ps_msg_count
HPRPST
8M
4M
2M
1M
low_limit
med_limit
high_limit
network_limit
HPRSESLM
NOLIMIT
sess_lim
DISABLED
(27)
HPRSTALL
0
timeout_limit
HSRTSIZE
9973
number_of_queue_pointers
INITDB
ALL
DIR
TOPO
NONE
(28)



Notes:

1 APPNCOS is meaningful only if the NODETYPE start option is also used.

2 BN is meaningful only if the NODETYPE=NN start option is also used.

3 BNDYN is meaningful only if the BN=YES start option is also used.

4 BNORD is meaningful only if the BN=YES start option is also used.

5 CDSERVR is meaningful only if the NODETYPE=NN start option is also used.

6 CDSREFER is meaningful only if the NODETYPE=NN and CDSERVR=NO start options are also used.

7 The CMPMIPS start option is meaningful only if the value for CMPVTAM is greater than 1.

8 CONNTYPE is meaningful only if the NODETYPE start option is also used.

9 CPCP is meaningful only if the NODETYPE start option is also used.

10 Specify the CSDUMP start option twice to set both message and sense code triggers.

11 DIRSIZE is meaningful only if the NODETYPE=NN start option is also used.

12 DIRTIME is meaningful only if the NODETYPE=NN start option is also used.

13 DLURSAW is meaningful only if the NODETYPE=NN start option is also used.

14 Because of the volume of messages that can be generated, it is not recommended that this option be enabled during normal operation. Instead, it is recommended that this option be enabled (using the MODIFY VTAMOPTS command) on all necessary hosts only when trying to diagnose specific problems. After the problem has been diagnosed or documentation has been collected, this option should be disabled once again (using the MODIFY VTAMOPTS command).

15 If the DSPLYMAX start option value is less than 100, that value is the default for DSPLYDEF.

16 DYNADJCP is meaningful only if the NODETYPE start option is also used.

17 Two character prefix.

18 EEHPRANR is meaningful only when the NODETYPE=NN start option is also used.

19 The EEVERIFY start option is meaningful only if VTAM provides RTP-level HPR support. The NODETYPE start option must be coded and the RTP value must be specified on the HPR start option.

20 ENCRYPTN=CCA needs to be coded when Triple Des Encryption is required.

21 The ENSEMBLE setting is used to either permit or deny connectivity to the intraensemble data network and the intranode management network. It does this by either allowing or denying activation of OSX and OSM interfaces.

22 HOSTNAME is meaningful only if the NODETYPE start option is also used. If neither HOSTNAME nor IPADDR is specified on any of the GROUP definition statements within the Enterprise Extender XCA major node, then either the HOSTNAME, TCPNAME, or IPADDR start options must be specified in order to activate an Enterprise Extender link. The HOSTNAME start option specifies the default hostname to be used for name-to-address resolution as part of activating an Enterprise Extender connection, and must resolve at this node to a static VIPA address associated with a TCP/IP stack at this node. If IPADDR is specified along with HOSTNAME on the START command, the IPADDR value is ignored.

23 HOSTSA specifies the subarea number of this VTAM. If HOSTSA is not coded, then a default subarea number of 1 is used.

24 HPR is meaningful only if NODETYPE is also used.

25 HPRCLKRT=ADAPTIVE is meaningful only in Enterprise Extender configurations that have a defined capacity of 1 Gb (gigabit) or higher access speeds.

26 This option is meaningful only if VTAM provides RTP-level HPR support.

27 HPRSESLM=DISABLED is meaningful only on interchange nodes.

28 INITDB is meaningful only if the NODETYPE=NN start option is also used.

29 When specifying an InOpCode for the second parameter, always specify three digits by including any leading zeros.

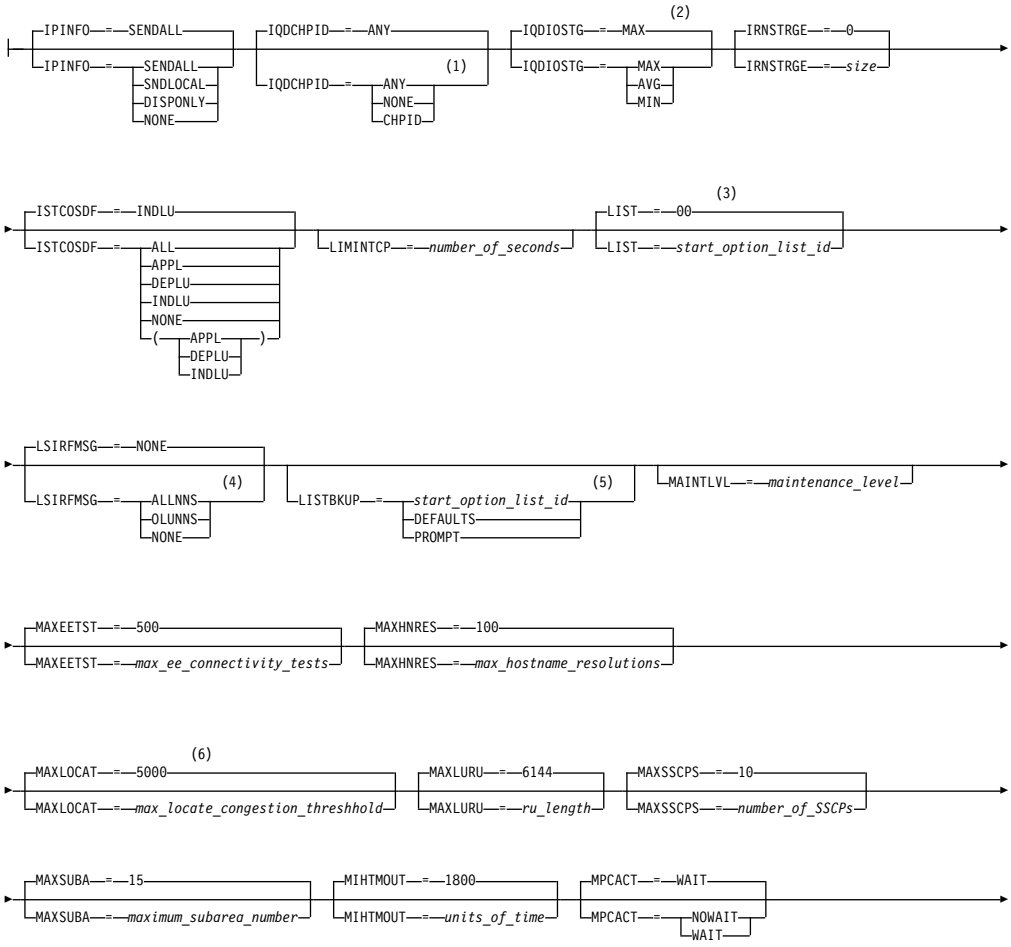
30 If an InOpCode is specified for the second parameter, the first parameter cannot be ALL.

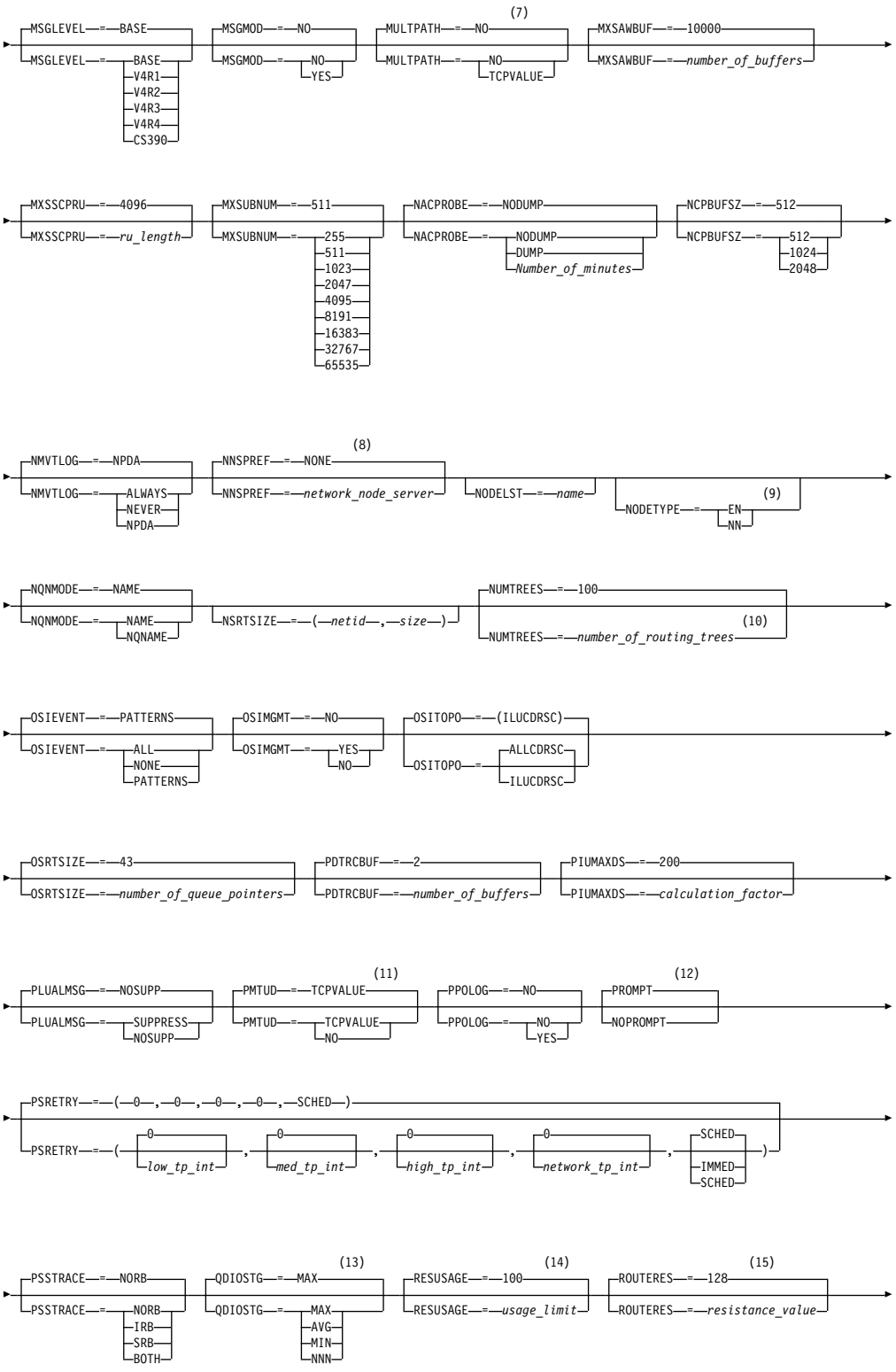
31 INOPCODE has no effect unless INOPDUMP is active for the resource when an inoperative condition is detected. See the MODIFY INOPCODE command for more details.

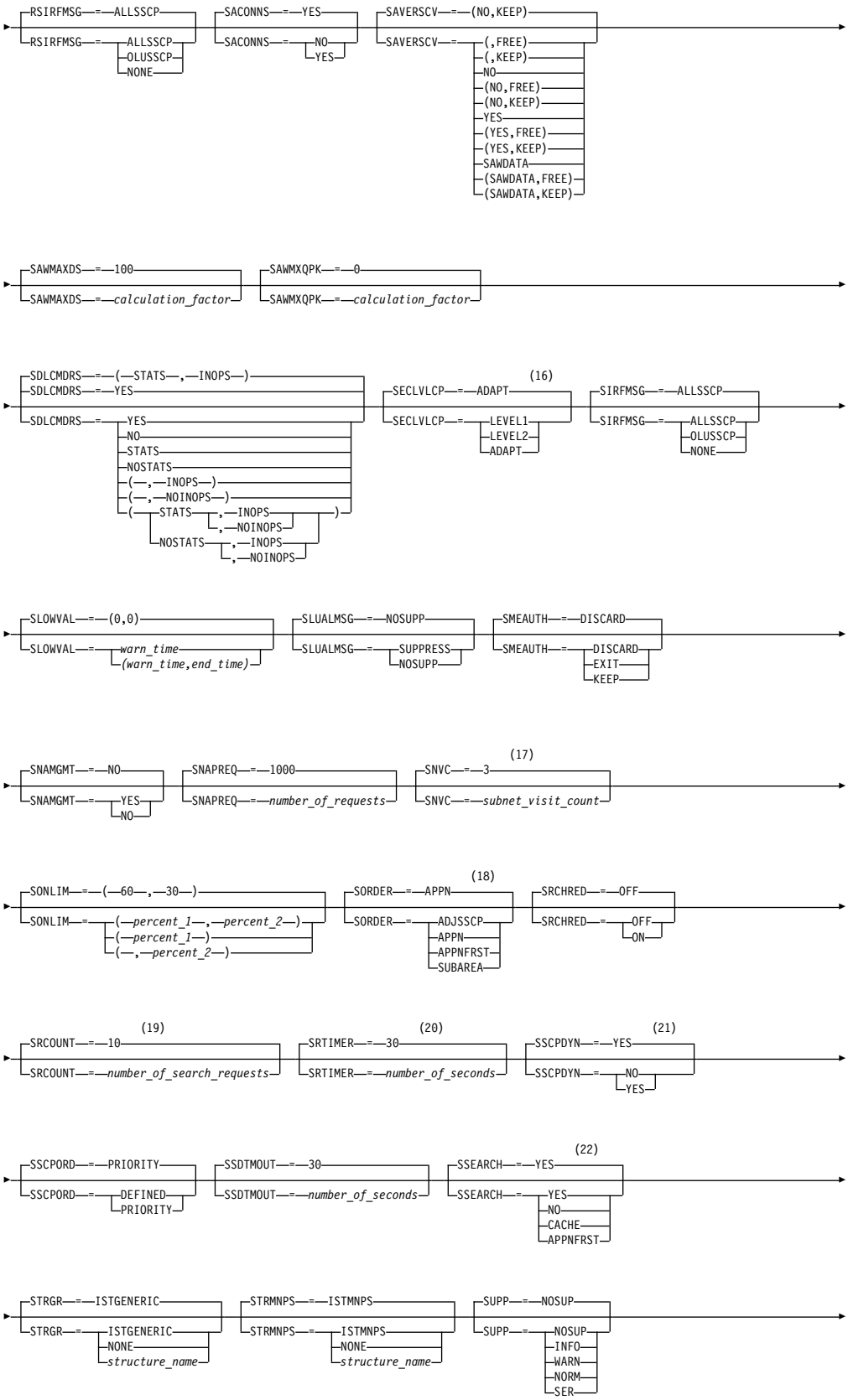
32 Multiple INOPCODE parameters can be specified by the START command, and will be processed left to right as they are entered. This is different from specifying the INOPCODE parameter on either the MODIFY INOPCODE command or the MODIFY VTAMOPTS command, where only one INOPCODE parameter is allowed for each entry of these commands.

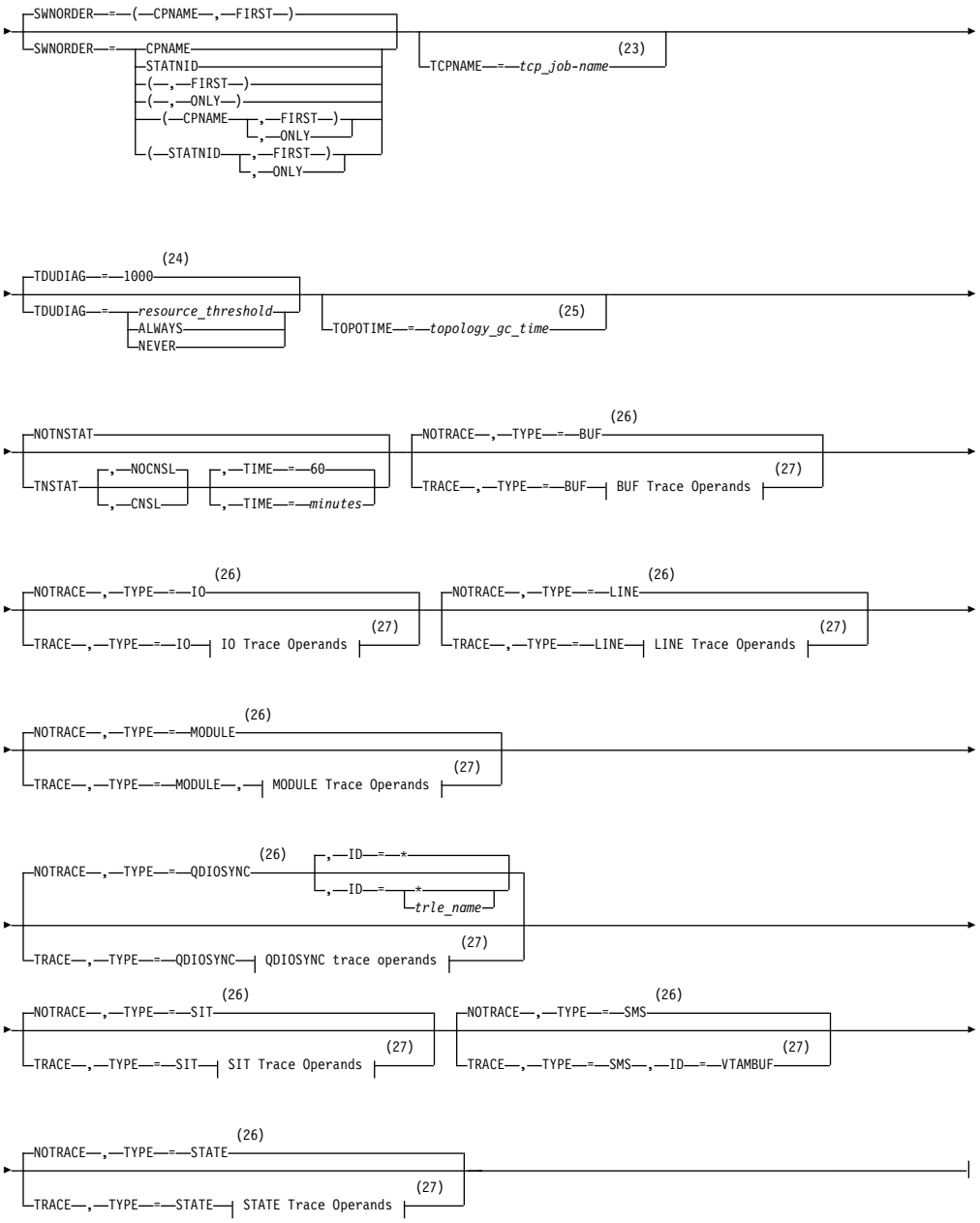
33 INOPDUMP status is propagated to resources that are defined within a TRLE when the entry is activated.

34 IPADDR is meaningful only if the NODETYPE start option is also used. If neither IPADDR nor HOSTNAME is specified on any of the GROUP definition statements within the Enterprise Extender XCA major node, then either the HOSTNAME, TCPNAME, or IPADDR start option must be specified in order to activate an Enterprise Extender link. The IPADDR start option specifies the default IPv4 or IPv6 static VIPA address to be used when activating an Enterprise Extender connection. If HOSTNAME is specified along with IPADDR on the START command, the IPADDR value is ignored.




MSGLEVEL
BASE
V4R1
V4R2
V4R3
V4R4
CS390
MSGMOD
NO
YES
(7)
MULTPATH
NO
TCPVALUE
MXSAWBUF
number_of_buffers
MXSSCPRU
4096
ru_length
MXSUBNUM
255
511
1023
2047
4095
8191
16383
32767
65535
NACPROBE
NODUMP
DUMP
Number_of_minutes
NCPBUFSZ
512
1024
2048
NMVTLOG
NPDA
ALWAYS
NEVER
(8)
NNSPREF
NONE
network_node_server
NODELST
name
(9)
NODETYPE
EN
NN
NQNMODE
NAME
NQNAME
NSRTSIZE
netid
size
NUMTREES
100
(10)
number_of_routing_trees
OSIEVENT
PATTERNS
ALL
NONE
OSIMGMT
YES
NO
OSITOPO
(ILUCDRSC)
ALLCDRSC
ILUCDRSC
OSRTSIZE
43
number_of_queue_pointers
PDTRCBUF
2
number_of_buffers
PIUMAXDS
200
calculation_factor
PLUALMSG
NOSUPP
SUPPRESS
(11)
PMTUD
TCPVALUE
PPOLOG
(12)
PROMPT
NOPROMPT
PSRETRY
SCHED
low_tp_int
med_tp_int
high_tp_int
network_tp_int
IMMED
PSSTRACE
NORB
IRB
SRB
BOTH
QDIOSTG
(13)
MAX
AVG
MIN
NNN
RESUSAGE
(14)
usage_limit
ROUTERES
(15)
resistance_value


RSIRFMSG = ALLSSCP
RSIRFMSG = ALLSSCP
OLUSSCP
NONE
SACONNS = YES
SACONNS = NO
YES
SAVERSCV = (NO,KEEP)
SAVERSCV = (,FREE)
(,KEEP)
NO
(NO,FREE)
(NO,KEEP)
YES
(YES,FREE)
(YES,KEEP)
SAWDATA
(SAWDATA,FREE)
(SAWDATA,KEEP)
SAWMAXDS = 100
SAWMAXDS = calculation_factor
SAWMXQPK = 0
SAWMXQPK = calculation_factor
SDLCMDRS = (STATS,INOPS)
SDLCMDRS = YES
SDLCMDRS = YES
NO
STATS
NOSTATS
(,INOPS)
(,NOINOPS)
(STATS,INOPS)
,NOINOPS
NOSTATS,INOPS
,NOINOPS
(16)
SECLVLCP = ADAPT
SECLVLCP = LEVEL1
LEVEL2
ADAPT
SIRFMSG = ALLSSCP
SIRFMSG = ALLSSCP
OLUSSCP
NONE
SLOWVAL = (0,0)
SLOWVAL = warn_time
(warn_time,end_time)
SLUALMSG = NOSUPP
SLUALMSG = SUPPRESS
NOSUPP
SMEAUTH = DISCARD
SMEAUTH = DISCARD
EXIT
KEEP
SNAMGMT = NO
SNAMGMT = YES
NO
SNAPREQ = 1000
SNAPREQ = number_of_requests
(17)
SNVC = 3
SNVC = subnet_visit_count
SONLIM = (60,30)
SONLIM = (percent_1,percent_2)
(percent_1)
(,percent_2)
(18)
SORDER = APPN
SORDER = ADJSSCP
APPN
APPNFRST
SUBAREA
SRCHRED = OFF
SRCHRED = OFF
ON
(19)
SRCOUNT = 10
SRCOUNT = number_of_search_requests
(20)
SRTIMER = 30
SRTIMER = number_of_seconds
(21)
SSCPDYN = YES
SSCPDYN = NO
YES
SSCPORD = PRIORITY
SSCPORD = DEFINED
PRIORITY
SSDTMOUT = 30
SSDTMOUT = number_of_seconds
(22)
SSEARCH = YES
SSEARCH = YES
NO
CACHE
APPNFRST
STRGR = ISTGENERIC
STRGR = ISTGENERIC
NONE
structure_name
STRMNPS = ISTMNPS
STRMNPS = ISTMNPS
NONE
structure_name
SUPP = NOSUP
SUPP = NOSUP
INFO
WARN
NORM
SER



Notes:

1 The IQDCHPID option controls which IQD CHPID (and related subchannel devices) VTAM selects to dynamically build the iQDIO (IUTIQDIO) MPC group. The IUTIQDIO MPC group is used for TCP/IP dynamic XCF communications within System z. Although this option can be modified (and the modification will immediately be displayed) while the IUTIQDIO MPC group is currently active, any modifications have the effects shown in the section called IQD CHPID modifications.

2 This option affects only iQDIO devices that use a MFS of 64k. The smaller frame sizes will always use 126 SBALs. You can override this option on a per-device basis using the READSTORAGE parameter on the LINK or INTERFACE statement in the TCP/IP profile. See z/OS Communications Server: IP Configuration Reference for more details.

3 LIST can be entered by a VTAM operator only. If LIST is coded in an ATCSTR*xx* file, it is considered to be an error and is ignored.

4 Because of the volume of messages that can be generated, it is not recommended that this option be enabled during normal operation. Instead, it is recommended that this option be enabled (using the MODIFY VTAMOPTS command) on all necessary hosts only when trying to diagnose specific problems. After the problem has been diagnosed or documentation has been collected, this option should be disabled once again (using the MODIFY VTAMOPTS command).

5 LISTBKUP can be coded only in a start option file. If you enter it on the START command or at an operator prompt, VTAM will ignore it.

6 MAXLOCAT is meaningful only if NODETYPE is specified.

7 MULTPATH is meaningful only if the NODETYPE start option is also specified.

8 NNSPREF can be specified only if NODETYPE=EN is specified during VTAM START processing.

9 NODETYPE enables APPN function. The combination of HOSTSA, NODETYPE, and SACONNS determines the configuration (subarea node, interchange node, migration data host, network node, or end node).

10 NUMTREES is meaningful only if the NODETYPE=NN start option is also used.

11 PMTUD is meaningful only if the NODETYPE start option is also specified.

12 A VTAM operator cannot enter the PROMPT or NOPROMPT start option; it can be coded only in ATCSTR00. The value coded in ATCSTR00 is ignored if start options are entered on the START command or if VTAM finds an error in a start list. Upon finding an error in a start list, VTAM prompts the operator so that the operator can specify the option correctly.

13 QDIOSTG defaults to MAX for 64-bit (z/Architecture) machines and MIN for non 64-bit machines. You can override this option on a per-device basis using the READSTORAGE parameter on the LINK or INTERFACE statement in the TCP/IP profile. See z/OS Communications Server: IP Configuration Reference for more details.

14 RESUSAGE is meaningful only if the NODETYPE=NN start option is also used.

15 ROUTERES is meaningful only if the NODETYPE=NN start option is also used.

16 The SECLVLCP start option is meaningful only if the NODETYPE and VERIFYCP start options are also used.

17 SNVC is meaningful only if the BN=YES start option is also used.

18 SORDER is meaningful only in an interchange node or a migration data host.

19 SRCOUNT is meaningful only if the SRCHRED=ON start option is also used.

20 SRTIMER is meaningful only if the SRCHRED=ON start option is also used.

21 The SSCPDYN start option applies only for interconnected networks (that is, GWSSCP=YES is used).

22 SSEARCH is meaningful only if the NODETYPE=NN start option is also used.

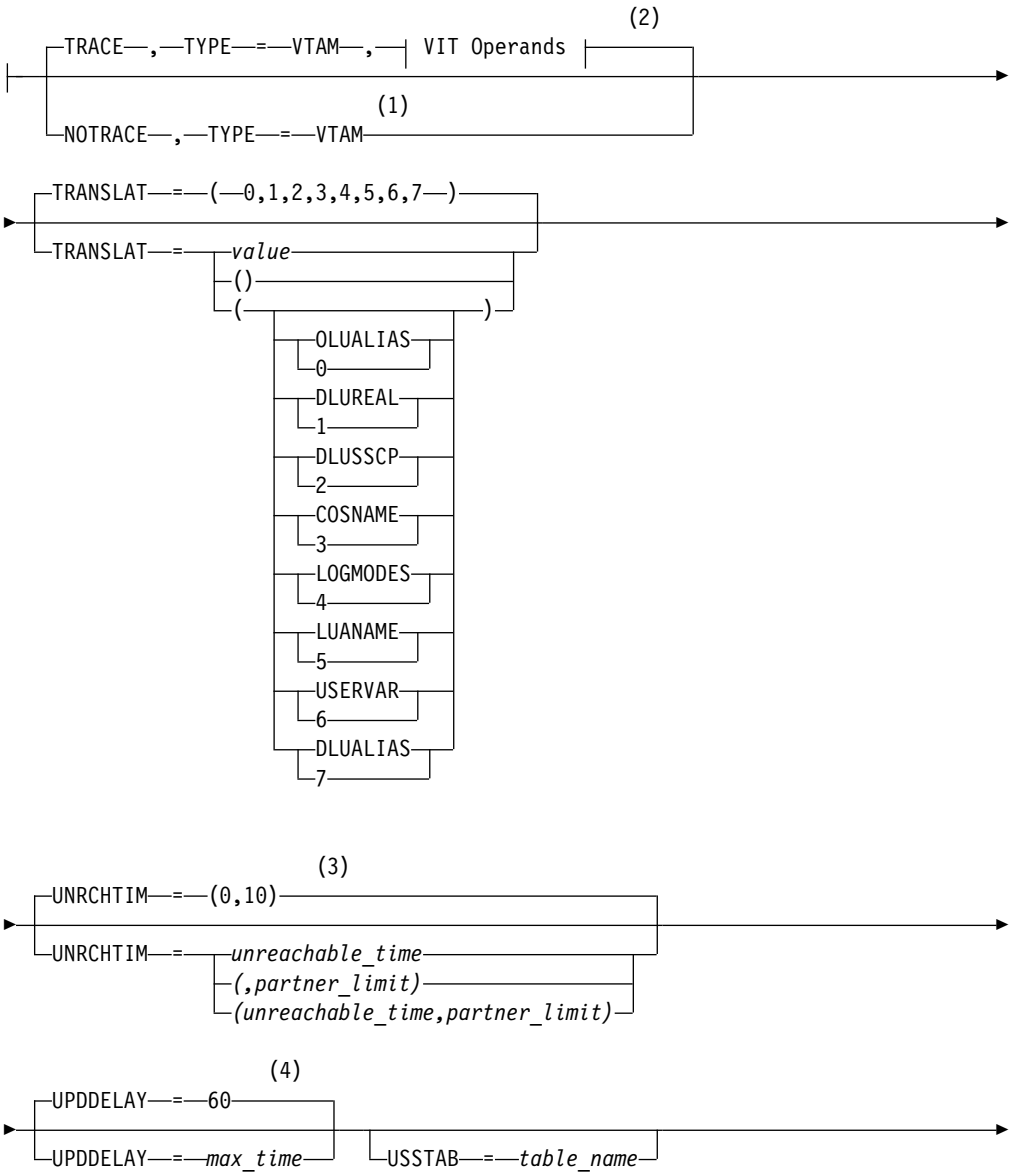
23 TCPNAME is meaningful only if the NODETYPE start option is also used. If neither IPADDR nor HOSTNAME is specified on any of the GROUP definition statements within the Enterprise Extender XCA major node, then either the HOSTNAME, TCPNAME, or IPADDR start options must be specified in order to activate an Enterprise Extender link.

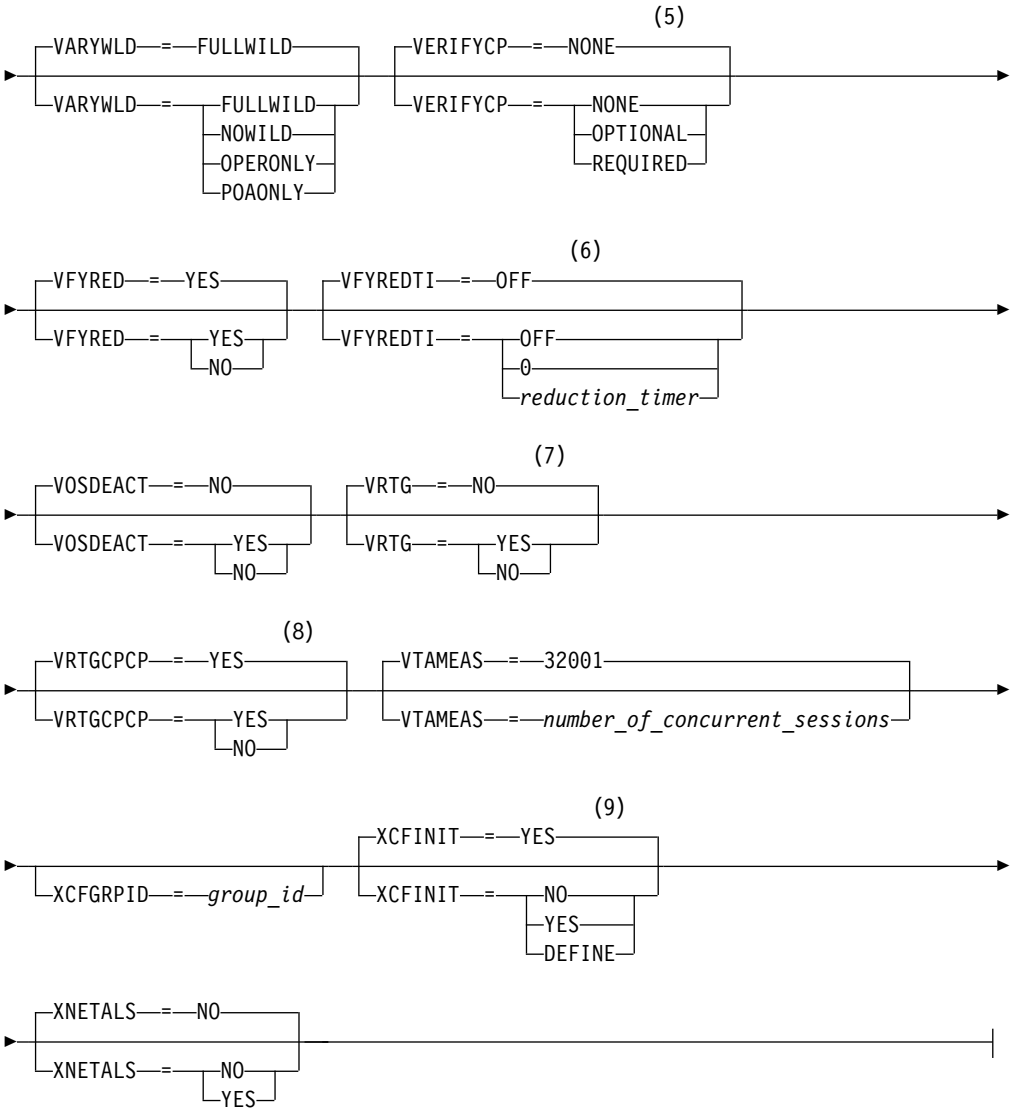
24 TDUDIAG is meaningful only if the NODETYPE=NN start option is also available.

25 TOPOTIME is meaningful only if the NODETYPE start option is also used.

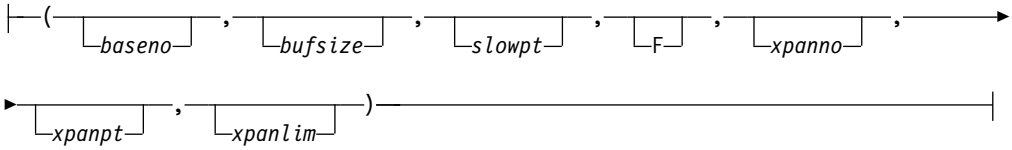
26 Do not use NOTRACE when starting VTAM, except to override a TRACE start option coded in a predefined list.

27 You can code TRACE and its qualifiers through position 71, even if you are in the middle of the start option. Continue the remainder of the item in the next record. Code the TYPE qualifier immediately after you code the TRACE start option.

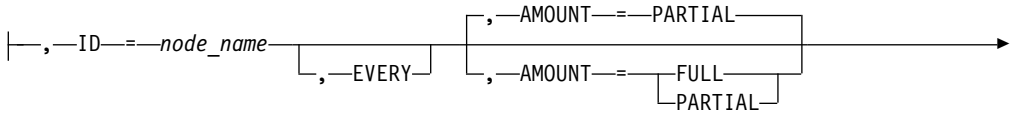


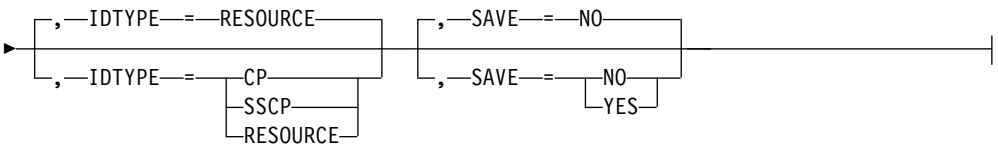


Buffer Pool Values:

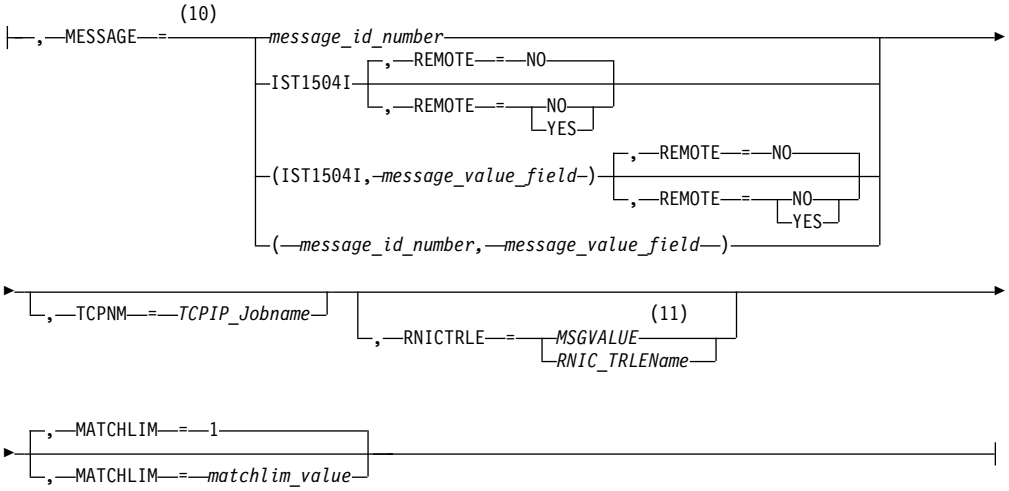


BUF Trace Operands:

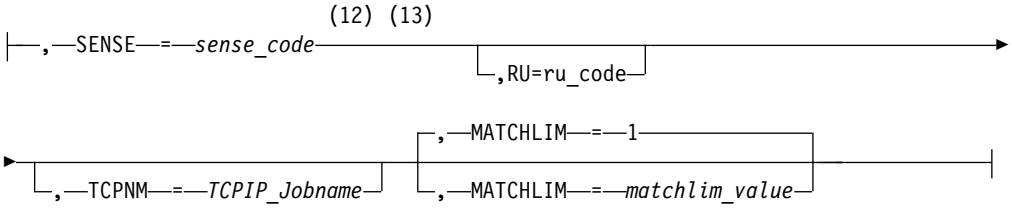




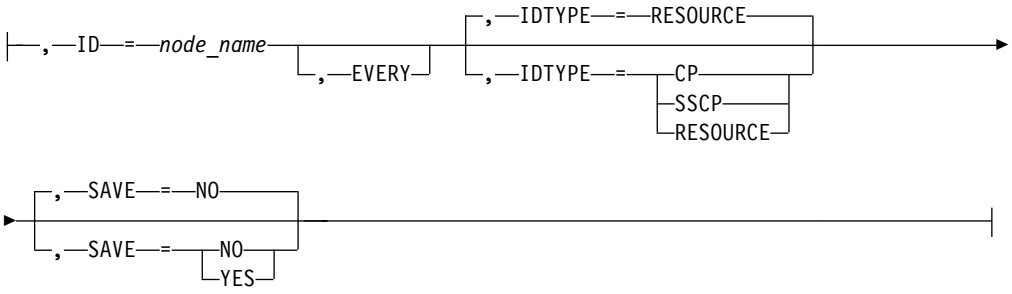
CSDUMP message trigger:



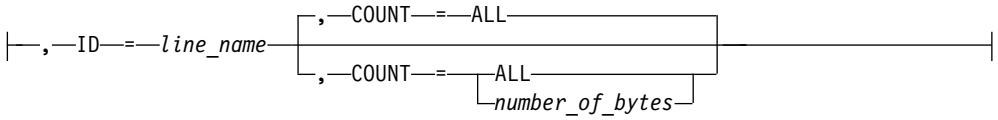
CSDUMP sense code trigger:



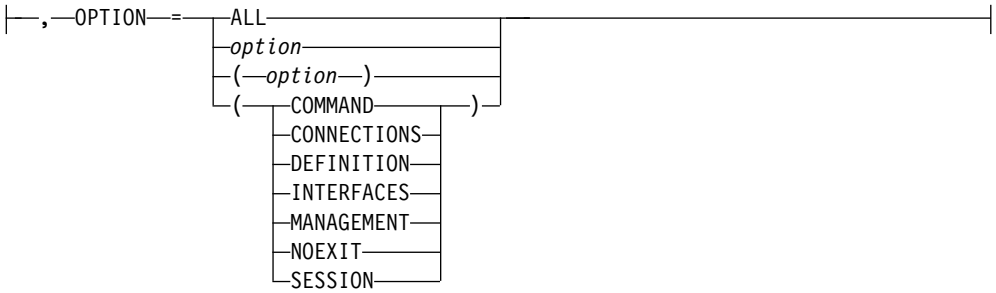
IO Trace Operands:



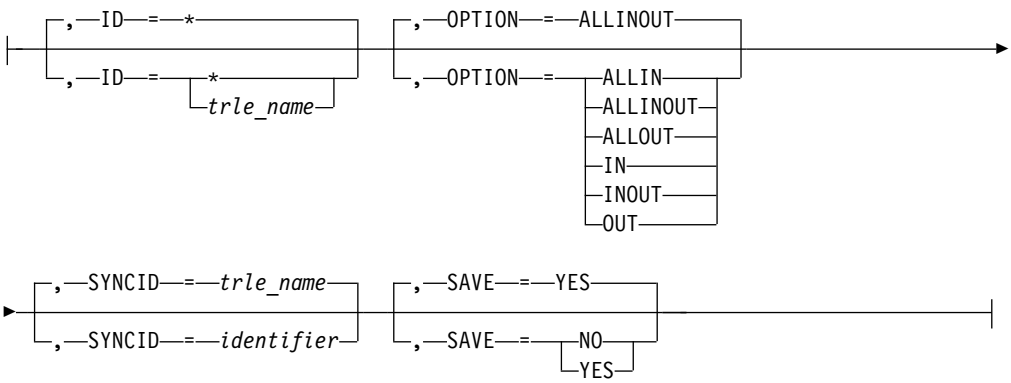
LINE Trace Operands:



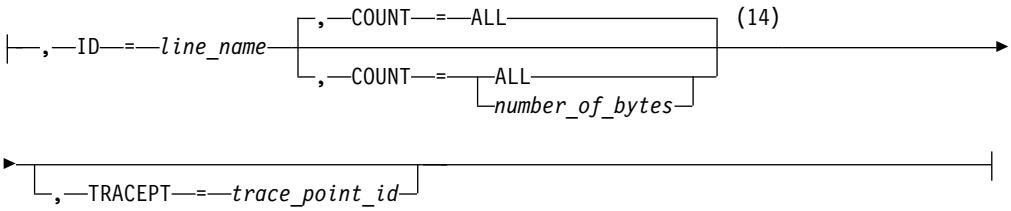
MODULE Trace Operands:



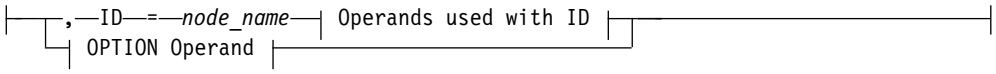
QDIOSYNC trace operands:



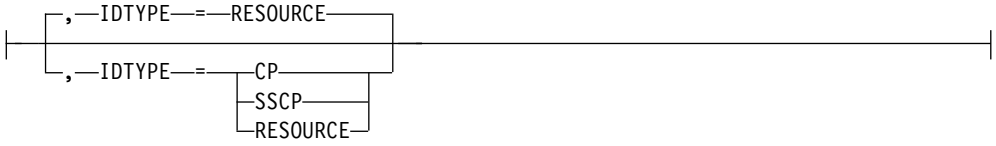
SIT Trace Operands:



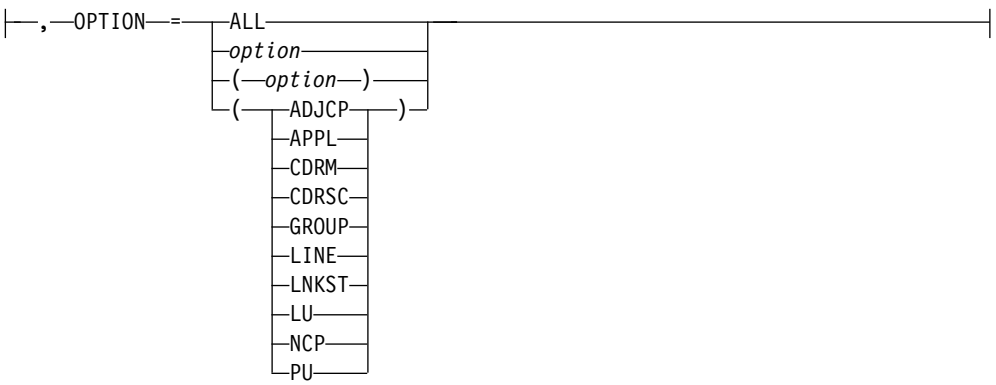
STATE Trace Operands:



Operands used with ID:



OPTION Operand:



Notes:

1 NOTRACE,TYPE=VTAM is accepted but ignored. Tracing is started with the default trace table size and the default options.

2 You can code TRACE and its qualifiers through position 71, even if you are in the middle of the start option. Continue the remainder of the item in the next record. Code the TYPE qualifier immediately after you code the TRACE start option.

3 UNRCHTIM is meaningful only if the NODETYPE start option is also used.

4 UPDDELAY is meaningful only if the OSIMGMT=YES start option is also used.

5 The VERIFYCP start option is meaningful only if the NODETYPE start option is also used.

6 VFYREDTI is meaningful only if the NODETYPE=NN start option is also used.

7 VRTG is meaningful only if the NODETYPE and HOSTSA start options are also used.

8 VRTGCPCP is meaningful only if the NODETYPE and HOSTSA start options are also used.

9 XCFINIT=YES is the default if VTAM is started as an APPN node (that is, the NODETYPE start option has been specified). XCFINIT=YES is not valid for pure subarea nodes. XCFINIT=DEFINE is the default if VTAM is started as a pure subarea node (the NODETYPE start option has not been specified).

10 When the same parameter is entered multiple times on a CSDUMP message trigger, only the last occurrence is accepted.

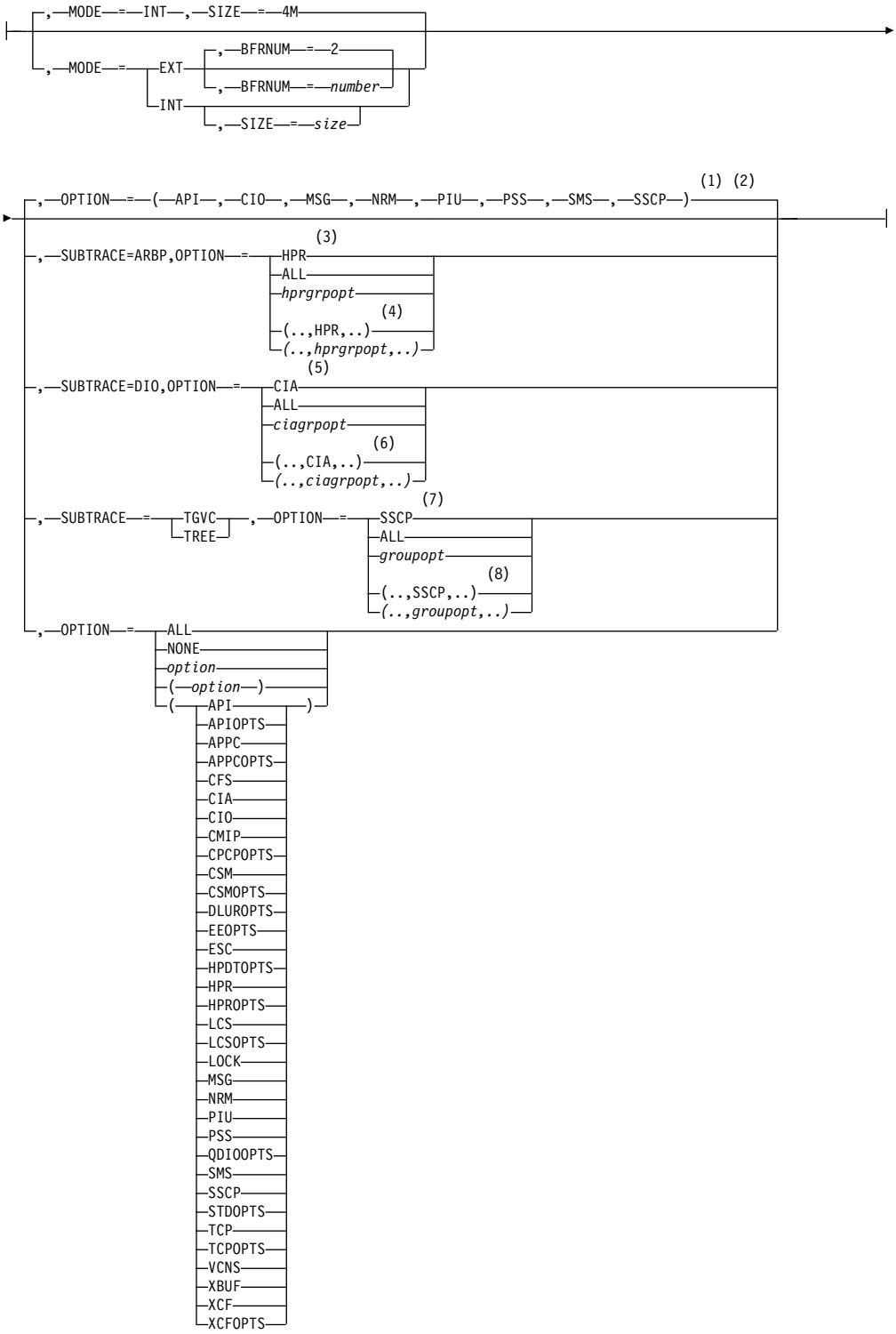
11 MSGVALUE is valid only when the MESSAGE operand is used and specifies either message IST2391I, IST2406I or IST2419I.

12 When an error message is received on any parameter of the CSDUMP start option, the remaining parameters for this CSDUMP start option are ignored. Enter the complete CSDUMP start option again when you are prompted.

13 When the same parameter is entered multiple times on a CSDUMP sense trigger, only the last occurrence is accepted.

14 COUNT applies only to the IBM 3720 and 3745 Communication Controllers.

VIT Operands:



Notes:

1 The default options apply only to MODE=INT.

2 PSS and SMS can be turned off.

3 When you specify SUBTRACE=ARBP and you code a single OPTION value,

the OPTION value must be HPR, ALL, or one of the group options (*hprgrpopt*) that include HPR as an individual option equivalent. The applicable group options are DLUROPTS, EEOPTS, HPDTOPTS, HPROPTS, QDIOOPTS, and XCFOPTS.

4 When SUBTRACE=ARBP is coded and you code multiple trace options in parentheses, you must code either HPR or one of the group options (*hprgrpopt*) that include HPR as an individual option equivalent inside the parentheses.

5 When you specify SUBTRACE=DIO and you code a single OPTION value, the OPTION value must be CIA, ALL, or one of the group options (*ciagrpopt*) that include CIA as an individual option equivalent. The applicable group options are EEOPTS, HPDTOPTS, HPROPTS, QDIOOPTS, TCPOPTS and XCFOPTS.

6 When SUBTRACE=DIO is coded and you code multiple trace options in parentheses, you must code either CIA or one of the group options (*ciagrpopt*) that include CIA as an individual option equivalent inside the parentheses.

7 When you code SUBTRACE=TGVC or SUBTRACE=TREE and you code a single OPTION value, the OPTION value must be either SSCP, ALL, or one of the group options (*groupopt*), all of which include SSCP as an individual option equivalent. The group options are APIOPTS, APPCOPTS, CPCPOPTS, CSMOPTS, DLUROPTS, EEOPTS, HPDTOPTS, HPROPTS, LCSOPTS, QDIOOPTS, STDOPTS, TCPOPTS, and XCFOPTS.

8 When you code SUBTRACE=TGVC or SUBTRACE=TREE and you code multiple trace options in parentheses, you must code either SSCP or one of the group options (*groupopt*) inside the parentheses.

Chapter 14. IP Messages: Volume 4 (EZZ, SNM)

EZZ0378I D...NETSTAT,DEVLINKS<,PNETID=|SMC><,INTFNAME=><,FORMAT=LONG|SHORT>

Explanation: This message is the result of the DISPLAY TCPIP,,HELP,DEVLINKS command and shows the format of the command.

System action: TCP/IP continues.

Operator response: For more information about the command, see z/OS Communications Server: IP System Administrator's Commands.

System programmer response: None.

Module: EZACDHLP

Procedure name: parseFile

EZZ4336I ERROR DURING *link_control_function* **INTERFACE** *interface_name* **- CODE** *error_code* **DIAGNOSTIC CODE** *internal_diagnostic_code*

Explanation: The Link Layer detected an error during activation of the interface.

link_control_function is the function that is being performed on the interface.

interface_name is the name of the interface.

error_code is the Data Link Control (DLC) status code for the link layer.

internal_diagnostic_code is an internal diagnostic code for use by IBM.

System action: If the *interface_name* value represents a RoCE or an internal shared memory (ISM) interface and the *link_control_function* value is ENABLE CALLS TO, an error occurred while TCP/IP was registering a VLAN ID with the IBM 10GbE RoCE Express feature or ISM device. The registration failure might be a device issue or result from the fact that the registration request exceeded the maximum number of VLAN IDs that can be registered with the device. The interface remains active, but any TCP connections that are established across this VLAN ID might not use Shared Memory Communications (SMC) processing.

In all other cases, TCP/IP deactivates the interface.

Operator response: If the last 4 digits of the error code are X'3016', the most likely reason for the error is that the TRLE definition for the interface is not active. In this case, activate the TRLE and restart the interface. Otherwise, inform the system programmer about the error.

System programmer response: See the z/OS Communications Server: IP and SNA Codes for information about Data Link Control (DLC) status codes for the link layer and perform the action described for the indicated status code. If applicable, correct the hardware problem and restart the interface.

Module: TCPIP

Procedure name: EZBIFIUT

EZZ8453I *jobtype* **STORAGE**

Explanation: TCP/IP issues this message as part of a group of messages in response to a DISPLAY TCPIP,*procname*,STOR command. This is the first message in the group. A complete description of the message group follows:

```
EZZ8453I jobtype STORAGE

EZZ8454I jobname STORAGE     CURRENT MAXIMUM  LIMIT
EZD2018I location
EZZ8455I         storagetype current maximum  limit
EZD2024I         type        current maximum
EZZ8459I DISPLAY TCPIP STOR COMPLETED SUCCESSFULLY
```

EZZ8453I

EZZ8453I

This message identifies the type of information shown in the message group.

jobtype is the type of job. Possible values are:

TCPIP
The job is a TCP/IP job.

TELNET
The job is a TN3270 job.

EZZ8454I

This message is a header message for EZZ8455I.

jobname is the job name associated with the procedure used to start the job.

EZD2018I

This message identifies the storage location for the storage described in the subsequent message EZZ8455I.

location is the location of the storage. Possible values are:

31-BIT
The storage is 31-bit storage located below the 2 GB bar.

64-BIT
The storage is 64-bit storage located above the 2 GB bar.

EZZ8455I

This message contains storage totals.

storagetype is the storage type. Possible values are:

ECSA
The amount of extended common storage area in use.

PRIVATE
The amount of pooled private storage in use.

ECSA MODULES
The amount of common storage in use for load modules loaded by dynamic LPA.

HVCOMMON
The amount of 64-bit common storage in use.

HVPRIVATE
The amount of 64-bit private storage in use.

TRACE HVCOMMON
The amount of 64 bit common storage that was obtained for tracing.

TRACE HVPRIVATE
The amount of 64 bit common storage that was obtained for tracing.

SMC-R FIXEDMEMORY
The amount of 64-bit private fixed storage in use for Shared Memory Communications over Remote Direct Memory Access (SMC-R). An instance of message EZZ8455I specifying SMC-R FIXEDMEMORY is only included in the message group if SMC-R is or was previously enabled for this TCP/IP stack by specifying the SMCR parameter on the GLOBALCONFIG profile statement.

SMC-D FIXEDMEMORY
The amount of 64-bit private fixed storage in use for Shared Memory Communications - Direct Memory Access (SMC-D). An instance of message EZZ8455I specifying SMC-D FIXEDMEMORY is included in the message group only if SMC-D is or was previously enabled for this TCP/IP stack by specifying the SMCD parameter on the GLOBALCONFIG profile statement.

current is the amount of storage currently allocated. The value ends with either K to indicate 1024 bytes or M to indicate 1048576 bytes. The *current* value for SMC-R FIXEDMEMORY is the sum of the SMC-R SEND MEMORY and SMC-R RECV MEMORY *current* values in message EZD2024I.

maximum is the maximum amount of storage ever allocated since the job was started. The value ends with either K to indicate 1024 bytes or M to indicate 1048576 bytes. The *maximum* value for SMC-R FIXEDMEMORY is the maximum amount of storage ever allocated for SMC-R send and receive buffers combined, but can be less than the sum of the *maximum* values in message EZD2024I for SMC-R SEND MEMORY and SMC-R RECV MEMORY.

limit is the storage limit that the job allows.

- When *jobtype* on EZZ8453I is TELNET, the storage does not have a limit.
- When *storagetype* is SMC-R FIXEDMEMORY, *limit* is defined using the SMCR FIXEDMemory keyword value on the GLOBALCONFIG profile statement. The FIXEDMemory value represents the limit for all SMC-R storage, regardless of whether it is used for send or receive buffers.
- When *storagetype* is SMC-D FIXEDMEMORY, *limit* is defined using the SMCD FIXEDMemory keyword value on the GLOBALCONFIG profile statement.
- Otherwise, *limit* is defined on the GLOBALCONFIG profile statement for TCP/IP.

The value ends with either K to indicate 1024 bytes or M to indicate 1048576 bytes, is NOLIMIT if the storage does not have a limit, or is N/A for SMC-R FIXEDMEMORY when the SMC-R function was previously enabled on this TCP/IP stack but is not currently enabled. See z/OS Communications Server: IP Configuration Reference for more information.

EZD2024I

- This message contains storage totals. This message is only included in the message group if SMC-R is or was previously enabled for this TCP/IP stack by specifying the SMCR parameter on the GLOBALCONFIG profile statement.
- *type* is the storage type. Possible values are:

  SMC-R RECV MEMORY
  The amount of 64-bit private storage allocated as SMC-R receive buffers for all SMC-R link groups associated with this TCP stack.

  SMC-R SEND MEMORY
  The amount of 64-bit private storage allocated for SMC-R send buffers by this TCP/IP stack.
- *current* is the amount of storage currently allocated. The value ends with either K to indicate 1024 bytes or M to indicate 1048576 bytes.
- *maximum* is the maximum amount of storage ever allocated since the job was started. The value ends with either K to indicate 1024 bytes or M to indicate 1048576 bytes.

EZZ8459I

This message is displayed when the DISPLAY TCPIP,procname,STOR command completed.

System action: The job continues.

Operator response: None.

System programmer response: None.

User response: Not applicable.

Problem determination: None.

Module: EZACDDSU

Routing code: 0

Descriptor code: 5, 8, 9

Automation: Not applicable.

Example:

EZZ8453I

```
EZZ8453I TCPIP STORAGE
EZZ8454I TCPCS    STORAGE            CURRENT   MAXIMUM     LIMIT
EZD2018I 31-BIT
EZZ8455I          ECSA                2701K     3156K   NOLIMIT
EZZ8455I          PRIVATE             8557K     8561K   NOLIMIT
EZZ8455I          ECSA MODULES        8639K     8639K   NOLIMIT
EZD2018I 64-BIT
EZZ8455I          HVCOMMON               1M        1M   NOLIMIT
EZZ8455I          HVPRIVATE             50M       50M   NOLIMIT
EZZ8455I          TRACE HVCOMMON      2048M     2048M   NOLIMIT
EZZ8455I          SMC-R FIXEDMEMORY     12M       16M       40M
EZD2024I            SMC-R SEND MEMORY    4M        4M
EZD2024I            SMC-R RECV MEMORY    8M       12M
EZZ8455I          SMC-D FIXEDMEMORY     12M       16M       40M
EZZ8459I DISPLAY TCPIP STOR COMPLETED SUCCESSFULLY
```

Chapter 15. SNA Messages

IST087I **TYPE =** *line_type*, **CONTROL =** *line_control*, **HPDT =** *hpdtvalue*

Explanation: This message is part of several different message groups that VTAM issues in response to DISPLAY ID or DISPLAY TRL commands.

line_type indicates the type of line and can be one of the following values:

LEASED
SWITCHED DIAL-IN
SWITCHED DIAL-OUT
SWITCHED DIAL-INOUT

line_control can be one of the following values:

BSC
Binary synchronous communication

CTCA
Channel-to-channel attached

ISM
Internal shared memory

MPC
Multipath channel

NCP
Channel-attached NCP

ROCE
Remote Direct Memory Access (RDMA) over Converged Ethernet

SDLC
Synchronous data link control

SS Start-stop

TCP
Transmission Control Protocol

USER
User-defined protocol

XCF
Cross-system coupling facility

hpdtvalue can be one of the following values:

YES
Indicates the connection is capable of performing channel I/O directly to or from communications storage manager (CSM) buffers.

NO Indicates the connection is not capable of performing channel I/O directly to or from communications storage manager (CSM) buffers.

NA
Is displayed when *line_control* is not MPC or when the connection is not active.

System action: Processing continues.

Operator response: None.

System programmer response: None.

IST1221I

Routing code: 8

Descriptor code: 5

IST1221I *chtyp* **DEV =** *device_address* **STATUS =** *status* **STATE =** *system_state*

Explanation: VTAM issues this message as part of a message group in response to:

- A DISPLAY ID command to identify the operational status of all **READ** and **WRITE** subchannels.
- A DISPLAY ID command for an MPC line or a transport resource list entry (TRLE).
- A DISPLAY TRL command for an active TRLE.

The message group varies if the TRLE is using the Queued Direct I/O (QDIO) interface to either an IBM OSA-Express Adapter or a HiperSockets device. If the message group is for a TRLE that is not using QDIO, the message group will look as follows:

This message group displays a TRLE that does not represent an OSA-Express adapter or HiperSockets interface.

```
 IST075I  NAME = nodename, TYPE = LINE
 IST486I  STATUS = currentstatus, DESIRED STATE = desiredstate
 IST087I  TYPE = line_type, CONTROL = line_control, HPDT = hpdtvalue
 IST1954I TRL MAJOR NODE = trl_major_node_name
 IST1715I MPCLEVEL = mpc_level MPCUSAGE = mpc_usage
 IST1717I ULPID = ulp_id
[IST2219I resource ACTIVATION WAITING FOR MINIMUM NUMBER OF DEVICES]
[IST1801I UNITS OF WORK FOR NCB AT ADDRESS stor_addr]
[IST1802I pn  CURRENT = cur  AVERAGE = avg  MAXIMUM = max]
[IST1577I HEADER SIZE = hpsize DATA SIZE = dsize STORAGE = storage]
 IST1221I chtyp DEV = device_address STATUS = status STATE = system_state
⋮
[IST1577I  HEADER SIZE = hpsize DATA SIZE = dsize STORAGE = storage]
[IST1221I chtyp DEV = device_address STATUS = status STATE = system_state]
⋮
 IST314I  END
```

Note: VTAM displays all **WRITE** subchannel addresses for *nodename* value, followed by all **READ** subchannel addresses for *nodename*. For TCP/IP channel DLC connections, there is only one **R/W** subchannel.
The following is an example of the message group if it is for a TRLE that uses QDIO:

```
 IST075I  NAME = nodename, TYPE = LINE
 IST486I  STATUS = currentstatus, DESIRED STATE = desiredstate
 IST087I  TYPE = line_type, CONTROL = line_control, HPDT = hpdtvalue
 IST1954I TRL MAJOR NODE = trl_major_node_name
 IST1715I MPCLEVEL = mpc_level MPCUSAGE = mpc_usage
[IST1716I PORTNAME = port_name LINKNUM = link_num OSA CODE LEVEL = code_level]
[IST2263I PORTNAME = port_name PORTNUM = port_num OSA CODE LEVEL = code_level]
[IST2337I CHPID TYPE = ch_type   CHPID = chpid_num  PNETID = network_id]
[IST2184I QDIOSYNC = ALLINOUT - SYNCID = TRAP01 - SAVED = YES]
[IST1577I HEADER SIZE = hpsize DATA SIZE = dsize STORAGE = storage]
 IST1221I chtyp DEV = device_address STATUS = status STATE = system_state

⋮
[IST1577I HEADER SIZE = hpsize DATA SIZE = dsize STORAGE = storage]
[IST1221I chtyp DEV = device_address STATUS = status STATE = system_state]
⋮
 IST924I  -------------------------------------------------------------
[IST1221I DATA  DEV = device_address STATUS = status STATE = system_state]
[IST1724I I/O TRACE = iotrc TRACE LENGTH = length]
[IST1717I ULPID = ulp_id ULP INTERFACE = ulp_interface]
[IST2309I ACCELERATED ROUTING ENABLED]
[IST2310I ACCELERATED ROUTING DISABLED]
[IST2331I QUEUE   QUEUE     READ             QUEUE                ]
[IST2332I ID      TYPE      STORAGE          STATUS               ]
[IST2205I ------  --------  ---------------  ---------------------]
[IST2333I qid     qtype     storage_amount   qstat                ]
[IST2305I NUMBER OF DISCARDED INBOUND READ BUFFERS = sbalcnt]
```

```
[IST2386I NUMBER OF DISCARDED OUTBOUND WRITE BUFFERS = wbufcnt]
[IST1757I PRIORITYx: congstate  PRIORITYx: congstate]
[IST1757I PRIORITYx: congstate  PRIORITYx: congstate]
[IST2190I DEVICEID PARAMETER FOR OSAENTA TRACE COMMAND = deviceid]
[IST1801I UNITS OF WORK FOR NCB AT ADDRESS stor_addr]
[IST1802I pn  CURRENT = cur  AVERAGE = avg  MAXIMUM = max]
IST924I  -------------------------------------------------------------
:
[IST1221I TRACE DEV = device_address STATUS = status STATE = system_state]
[IST1724I I/O TRACE = iotrc TRACE LENGTH = length]
[IST1717I ULPID = ulp_id ULP INTERFACE = ulp_interface]
[IST2319I IQD NETWORK ID = netid]
[IST2309I ACCELERATED ROUTING ENABLED]
[IST2310I ACCELERATED ROUTING DISABLED]
[IST2331I QUEUE   QUEUE     READ             QUEUE                ]
[IST2332I ID      TYPE      STORAGE          STATUS               ]
[IST2205I ------  --------  ---------------  ----------------------]
[IST2333I qid     qtype     storage_amount   qstat                ]
[IST2305I NUMBER OF DISCARDED INBOUND READ BUFFERS = sbalcnt]
[IST2386I NUMBER OF DISCARDED OUTBOUND WRITE BUFFERS = wbufcnt]
[IST1757I PRIORITY1: congstate  PRIORITY2: ****NA****]
[IST1757I PRIORITY3: ****NA****  PRIORITY4: ****NA****]
 IST1801I UNITS OF WORK FOR NCB AT ADDRESS stor_addr
IST1802I pn  CURRENT = cur  AVERAGE = avg  MAXIMUM = max
[IST924I  -------------------------------------------------------------]
:
 IST314I  END
```

Note: VTAM displays all **WRITE** subchannel addresses for the node specified by the *nodename* value, followed by all **READ** subchannel addresses for that node, followed by all **DATA** subchannel addresses, followed by all **TRACE** subchannel addresses. DATA subchannel addresses and TRACE subchannel addresses are displayed only for an OSA-Express TRLE. For each DATA and TRACE subchannel address that is currently being used by an upper-layer protocol (ULP), the name of the z/OS Communications Server ULP (for example, the TCP/IP procedure name) using that data subchannel is displayed.

IST075I

In the message text:

nodename
The name of the resource that was entered on the DISPLAY ID command.

nodetype
The resource type of the major or minor node. The *nodetype* value is always **LINE** for this message group.

IST087I

In the message text:

line_type
The type of line. The *line_type* value is always **LEASED** for this message group.

line_control
The *line_control* value is always **MPC** (multipath channel) for this message group.

hpdtvalue
The *hpdtvalue* can be one of the following:

YES
Indicates the connection is capable of performing channel I/O directly to or from communications storage manager (CSM) buffers.

NO Indicates the connection is not capable of performing channel I/O directly to or from communications storage manager (CSM) buffers.

NA
Is displayed when the connection is not active.

IST486I

In the message text:

currentstatus
The current status of the node. See the z/OS Communications Server: IP and SNA Codes for status information.

desiredstate
The node state that is desired. See the z/OS Communications Server: IP and SNA Codes for status information. If VTAM cannot determine the desired state, *desiredstate* is ***NA***.

IST1221I

In the message text:

chtyp
The type of subchannel. Possible values are READ, WRITE, R/W, DATA, or TRACE

device_address
The hexadecimal address of the subchannel that is displayed.

status
The condition or state of the subchannel that is displayed. Possible values are:

ACTIVE
Subchannel is active.

INOP Subchannel path is inoperative.

RESET Subchannel path is not ready.

SLOWDN
Subchannel path is in slowdown mode.

ACTPEND
DLC is in the process of activating.

OPEN.PEND
DLC is in the process of opening a connection.

IDX.PEND
DLC is in the process of IDXINIT transmission for a DATA channel.

START.PEND
DLC is in the process of starting data flow for a connection.

INACT.PEND
DLC is in the process of deactivating.

system_state
The *system_state* value can be one of the following:

ONLINE
An MVS VARY ONLINE command for the subchannel has completed successfully and the channel is now available for use.

OFFLINE
An MVS VARY OFFLINE command has been issued for the subchannel and the command has completed successfully. The subchannel is no longer available for use.

PEND_OFFLINE
An MVS VARY OFFLINE command has been issued for the subchannel and the subchannel is in the process of completing the command.

N/A The system state cannot be determined for DATA subchannel addresses. This state is also displayed in cases where VTAM has not allocated or could not allocate the UCB for the subchannel.

Tip: If the MVS status of the subchannel is required, you can use the D U,xxxx command, where xxxx is the subchannel address.

IST1577I

This message is displayed only when HPDT=YES in message IST087I. This message is not displayed if the TRLE is IUTSAMEH, which is the TRLE for same-host communication.

In the message text:

hpsize
The MPC header segment size, in bytes.

dsize
The maximum MPC data segment size, in kilobytes.

storage
The storage medium that is used for inbound data (on READ subchannels). Possible values are:

ECSA
An extended common service area buffer provided by the communications storage manager (CSM).

DATASPACE
A data space buffer provided by the communications storage manager (CSM).

*****NA*****
Not applicable. This value is issued for WRITE subchannels.

IST1715I

In the message text:

mpc_level
The level of MPC connection. Possible values are:

HPDT
Indicates that the connection is capable of performing channel I/O directly to or from communications storage manager (CSM) buffers.

NOHPDT
Indicates that the connection is not capable of performing channel I/O directly to or from communications storage manager (CSM) buffers.

QDIO
(Queued Direct I/O) Indicates that the connection performs channel I/O operations using direct IO instead of CCW channel operations. The connection is also HPDT capable, and can therefore perform the direct IO to or from communications storage manager (CSM) buffers.

mpc_usage
Indicates whether the MPC connection can be used exclusively by only one ULP, or shared by multiple ULPs. Possible values are:

SHARE
Indicates that the connection can be shared by multiple ULPs.

EXCLUSIVE
Indicates that the connection can only be used by the first ULP that requests usage of the MPC connection.

IST1716I

This message is displayed only for TRLEs representing an IBM OSA-Express Adapter or an IBM Open Systems Adapter used for native access to an ATM network.

In the message text:

port_name
The port name to be assigned to the port on the IBM Open Systems Adapter. Each IBM Open Systems Adapter has one *port_name* that is represented by one TRLE.

link_num
The relative adapter number of the OSA-Express Adapter port represented by this TRLE. For an IBM Open Systems Adapter used for native access to an ATM network, the *link_num* value is N/A.

code_level
The OSA processor code level of the OSA-Express. For some versions of OSA-Express, the *code_level* value is N/A. For detailed instructions about setting up an OSA-Express feature, see the zEnterprise System and System z10 OSA-Express Customer's Guide and Reference.

IST1717I

This message is displayed for all TRLEs that are currently being used by at least one ULP. A separate IST1717I message will be displayed for each ULP using this TRLE. For a dynamic TCP TRLE, or an exclusively owned TRLE, only one message with ULPID will be issued, because there can only be one ULP using each of these TRLEs. For an OSA-Express Adapter, one message with ULPID will be issued for each Datapath channel address in use by a ULP. For other TRLEs, more than one ULPID message might be issued, depending on how many upper-layer protocols are using the TRLE.

In the message text:

ulp_id
The name of a z/OS Communications Server upper-layer protocol (ULP) that is using the TRLE or using one of the datapath channels of an OSA-Express TRLE.

- For TCP/IP ULPs, the *ulp_id* value is the TCPIP job name.
- For ANNC ULPs, the *ulp_id* value is the SNA PU name.
- For ATM or EE ULPs, the *ulp_id* value is the XCA major node name.

For all TRLEs with MPCLEVEL = QDIO, IST1717I will also display the interface dedicated to this datapath channel address. For all TRLEs whose MPCLEVEL is not QDIO, the ulp_interface will be *NA*.

ulp_interface
The name of either the interface or the device that is using one of the datapath channels of an OSA-Express TRLE.

IST1724I

This message is issued in response to DISPLAY ID or DISPLAY TRL commands. This message appears for a TRLE representing an OSA-Express adapter.

In the message text:

iotrc
Specifies whether I/O Trace is active for this OSA-Express data device (ON or OFF).

length
Specifies the number of bytes being recorded for I/O Trace for this OSA-Express data device.

For information about setting up an OSA-Express feature, see zEnterprise System and System z10 OSA-Express Customer's Guide and Reference.

IST1757I

This message is issued in response to DISPLAY ID or DISPLAY TRL commands. This message will appear for a TRLE representing an OSA-Express Adapter.

In the message text:

x The write priority level.

congstate
The congestion state of that priority level. The *congstate* value is **CONGESTED** when, at least once in the last congestion reporting window, all 128 writes for the priority level were unavailable. Otherwise *congstate* will be **UNCONGESTED**.

IST1954I

In the message text:

trl_major_node_name
The name of the TRL major node defining the TRLE.

IST2184I

This message is displayed for only a TRLE that represents an OSA-Express2 or later adapter and only when the OSA-Express2 or later adapter is armed for QDIOSYNC. See QDIOSYNC trace in z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for a description of the QDIOSYNC trace function.

In the message text:

armstate
The OPTION operand value from the MODIFY TRACE command or TRACE start option.

Tip: The OSA might be collecting more than what is specified by the *armstate* value while OSA merges the options for all Armed data devices.

Possible values are:

ALLIN
OSA is collecting inbound diagnostic data for all devices.

ALLINOUT
OSA is collecting inbound and outbound diagnostic data for all devices.

ALLOUT
OSA is collecting outbound diagnostic data for all devices.

IN OSA is collecting inbound diagnostic data for devices defined to this VTAM.

INOUT
OSA is collecting inbound and outbound diagnostic data for devices defined to this VTAM.

OUT
OSA is collecting outbound diagnostic data for devices defined to this VTAM.

syncid
The SYNCID operand value from the MODIFY TRACE command or TRACE start option. This value is to be used as part of a correlator when the OSA-Express2 or later diagnostic data is captured.

saved_state
The SAVE operand value from the MODIFY TRACE command or TRACE start option. Valid values are YES or NO.

IST2190I

This message is issued in response to DISPLAY ID or DISPLAY TRL commands for a TRLE configured with an MPCLEVEL parameter value of QDIO representing an OSA-Express adapter. This message appears for each active datapath channel if the OSA supports the OSA-Express network traffic analyzer (OSAENTA) trace function. The message displays the DEVICEID parameter, a number that uniquely identifies this datapath channel to the OSA-Express adapter. When a TCP/IP stack is performing the OSAENTA trace function for this OSA, this DEVICEID parameter can be specified on a TCP/IP OSAENTA profile configuration statement or a VARY TCPIP,,OSAENTA command to limit the tracing to just the user of this data device. See OSA-Express network traffic analyzer trace in z/OS Communications Server: IP Configuration Guide for more information about the OSAENTA trace function.

In the message text:

deviceid
The form *cs-mf-cl-us*, where

cs is the Channel subsystem ID for this data path device.

mf is the LPAR multiple image facility ID for the LPAR using this datapath device.

cl is the control unit logical identifier for this datapath device.

ua is the unit address for this data path device.

Each identifier is a 2 digit hexadecimal value in the range 00-FF.

IST2219I

This message is issued if the *resource* value defines an MPC channel-to-channel group, the activation of which is presently suspended waiting for the minimum required number of read and write devices to become available.

In the message text:

resource
The name of the TRLE or MPC subarea line that defines the MPC group.

IST2263I

This message is displayed if either of the following scenarios is true:

- PORTNUM is specified on the QDIO TRLE definition statement.
- VTAM detected it is connected to an IBM OSA-Express3 or later feature in QDIO mode.

In the message text:

port_name
The port name to be assigned to the port on the IBM Open Systems Adapter. Each IBM Open Systems Adapter has one port name that is represented by one TRLE.

port_num
The OSA-Express3 or later physical port number to be used for this QDIO MPC group. For OSA-Express2 and earlier or later adapters, only one physical port is available, so the *port_num* value will be 0.

code_level
The OSA processor code level of the OSA-Express. For some versions of OSA-Express, the *code_level* value will be N/A.

IST2305I

This is issued in response to DISPLAY NET,ID=*trlename* or DISPLAY NET,TRL,TRLE=*trlename* commands when the TRLE represents HiperSockets or an OSA-Express adapter.

In the message text:

sbalcnt
The number of storage block address lists (SBAL) that have been discarded since the activation of the device.

IST2309I

This message indicates that the upper-layer protocol (ULP) that is using the datapath channel of the OSA-Express or HiperSockets TRLE is using accelerated routing. If the ULP is a TCP/IP stack, then you can display the accelerator routing table by issuing the Netstat ROUTe/-r command with the QDIOACCEL modifier for a particular TCP/IP stack. For details about how to display the accelerator routing table, see the Netstat ROUTe/-r report in z/OS Communications Server: IP System Administrator's Commands.

IST2310I

This message indicates that the upper-layer protocol (ULP) that is using the datapath channel of the OSA-Express or HiperSockets TRLE is not using accelerated routing.

IST2319I

This message is issued if the TRLE that is displayed represents an IBM iQDIO Adapter (CHPID).

In the message text:

netid
The internal QDIO (IQD) Network ID is an internal system generated identifier that represents the internal logical network. The ID is associated with the IQD CHPID and can span the entire central processor complex (CPC), based on the system configuration of the IQD CHPID. Operating Systems that are running on this CPC, which are connected to the same IQD Network ID, are using the same internal logical network and therefore have network connectivity. The ID is subject to change during a power-on reset of the CPC, or with dynamic I/O updates for the IQD CHPID.

IST2331I

This message is the first of two header messages for the information displayed in message IST2333I.

IST2332I

This message is the second of two header messages for the information displayed in message IST2333I.

IST2333I

When OSA Express supports QDIO inbound workload queueing, z/OS Communications Server can initialize multiple input queues. IST2333I is displayed once for each initialized read queue.

In the message text:

qid
The queue identifier of the read queue. The *qid* value is in the form RD/*qid*. RD/1 represents the primary read queue and RD/2 through RD/8 represent any initialized ancillary read queues.

qtype
The queue type for this read queue. Possible values are PRIMARY, BULKDATA, EE, IPSEC, or SYSDIST.

storage_amount
The amount of storage defined by the VTAM start option QDIOSTG (or IQDIOSTG for iQDIO data devices). The VTAM start option value can be overridden on an individual device basis when READSTORAGE is configured on the LINK or INTERFACE statement in the TCP/IP profile.

A *storage_amount* value of ***NA*** appears if the *qstat* value is not ACTIVE. The queue has no read buffers and cannot be used by OSA Express to present inbound data.

The *storage_amount* value is displayed both in megabytes and in the number of QDIO read buffers that are storage block access lists (SBALs) that VTAM will use for this data device for inbound (read) processing. The *storage_amount* value is in the following format:

```
n.nM(nnn SBALS)
```

where *n.n* is the amount of storage in megabytes and *nnn* is the number of SBALs.

For an OSA-Express in QDIO mode, the size of an SBAL is fixed at 64 KB. For an iQDIO (HiperSockets) device, the SBAL size is variable. The iQDIO SBAL size is configured in a hardware configuration definition (HCD) when the maximum frame size (MFS) is specified. The default MFS is 16 KB, and the values 24 KB, 40 KB, and 64 KB are also supported. For an iQDIO device, both the VTAM start option IQDIOSTG and TCP/IP profile LINK or INTERFACE statement parameter READSTORAGE have an effect only when an MFS of 64 KB was configured.

qstat
The status of this read queue. Possible values are:

ACTIVE
The queue type is initialized and currently in use by the TCP/IP stack.

INITIALIZATION FAILURE
The queue type failed to initialize and will not be used by the TCP/IP stack.

NOT IN USE
The queue type is not currently in use by the TCP/IP stack.

NOT SUPPORTED BY OSA
The queue type is not supported by the OSA-Express adapter and will not be used by the TCP/IP stack.

IST2337I

This message is issued in response to DISPLAY NET,ID=*trlename* or DISPLAY NET,TRL,TRLE=*trlename* commands when the TRLE represents HiperSockets or an OSA-Express adapter.

In the message text:

chpid_type
The type of channel path identifier (CHPID) used by this TRLE:

OSD
Channel type for an OSA-Express CHPID configured in QDIO mode.

OSM
Channel type for an OSA-Express CHPID configured for attachment to the intranode management network.

OSX
Channel type for an OSA-Express CHPID configured for attachment to the intraensemble data network.

IQD
Channel type for HiperSockets (Internal Queued Direct I/O) communications.

chpid_num
The hexadecimal channel path identifier (CHPID) for the OSA adapter or HiperSockets device.

network_id
The physical network identifier.

- When *chpid_type* is OSX, *network_id* is always **IEDN**.
- When *chpid_type* is OSD or IQD, *network_id* is either the configured network identifier of the adapter, or ****NA**** if no network identifier was configured for the adapter.
- For all other *chpid_type* values, *network_id* is ****NA****.

IST2386I

This message is issued in response to DISPLAY NET,ID=*trlename* or DISPLAY NET,TRL,TRLE=*trlename* commands when the TRLE represents HiperSockets or an OSA-Express adapter.

In the message text:

wbufcnt
The number of outbound write buffers that have been discarded since the activation of the device.

System action: Processing continues.

Operator response: For MPC or TRLE configurations defined with multiple READ and multiple WRITE devices, MPC dynamics enables an operator to dynamically add and remove subchannels to and from the MPC/TRLE group.

- If a READ or WRITE MPC or TRLE subchannel displays as OFFLINE, issue an MVS ONLINE command (for example, VARY cua,ONLINE) to dynamically add the device back to the MPC or TRLE group.
- If a READ or WRITE MPC or TRLE subchannel displays as ONLINE, and you want to remove the subchannel from the group, issue the MVS OFFLINE command (for example, VARY cua,OFFLINE) to dynamically remove the device from the MPC or TRLE group.

Restriction: For subarea MPC connections, the MPCDYN=YES operand must be coded on the MPC GROUP or LINE definition to enable MPC dynamics.

System programmer response: For message IST2333I, use the *storage_amount* value to confirm the system storage use and to tune the performance of a specific data device.

Routing code: 2

Descriptor code: 5

IST1314I TRLE = *trl_element* STATUS = *trle_status* CONTROL = *lnctl*

Explanation: VTAM issues this message as part of a message group in response to any of the following commands:

- A DISPLAY ID command for a PU that supports an APPN host-to-host connection.
- A DISPLAY ID command for a PU that supports an XCF connection.
- A DISPLAY TRL command when the TRLE operand is not specified.

trl_element is the name of an element in the active transport resource list (TRL).

When *lnctl* is TCP, the name of the TRL element (TRLE) given by *trl_element* is dynamically generated by VTAM. The first three characters of the name are always **IUT** and the fourth character of the name indicates the device type according to the following list:

C CDLC

H Hyperchannel

L LCS

S Samehost

W CLAW

X CTC

When *lnctl* is ROCE, the name of the TRLE given by *trl_element* is dynamically generated by VTAM. The first three characters of the name are always **IUT**, the fourth character represents the port number (1 or 2), and the last four characters represent the Peripheral Component Interconnect Express (PCIe) function ID (PFID) used by the IBM 10GbE RoCE Express feature represented by *trl_element*.

When *lnctl* is ISM, the name of the TRLE given by *trl_element* is dynamically generated by VTAM. The first four characters of the name are always **IUT0**, and the last four characters represent the PFID used by the internal shared memory (ISM) device represented by *trl_element*.

trle_status is the resource status code that indicates the current status of the TRL element. If *trle_status* is ****NA****, then the TRL major node with the TRLE named on the PU definition must be activated. See Resource Status Codes and Modifiers inz/OS Communications Server: IP and SNA Codes for a description of these status codes.

lnctl is the line control setting for *trl_element*, and can be one of the following:

ISM
internal shared memory

MPC
multipath channel

ROCE
RDMA (Remote Direct Memory Access) over Converged Ethernet

TCP
transmission control protocol

XCF
cross-system coupling facility

System action: Processing continues.

Operator response: None.

System programmer response: None.

Routing code: 2

Descriptor code: 5

IST1451I TRLE = trlename TNSTAT = status

Explanation: VTAM issues this message as part of the response to the DISPLAY TNSTAT, MODIFY TNSTAT and MODIFY NOTNSTAT commands.

trlename is the name of the TRLE for which status is being reported.

status indicates the results of the MODIFY command or the status of tuning statistics recording for *trlename*.

- When *status* is ACTIVE, tuning statistics are currently being recorded for the devices in the TRLE.
- When *status* is INACTIVE, tuning statistics are not currently being recorded for the devices in the TRLE.
- When *status* is FAILED, VTAM does not support collection of tuning statistics for the TRLE specified as *trlename* on the MODIFY command. See Gathering tuning statistics in z/OS Communications Server: SNA Network Implementation Guide for more information.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Routing code: 2

Descriptor code: 5

IST1717I ULPID = *ulp_id* ULP INTERFACE = ulp_interface

Explanation: This message is issued in these different situations:

- As part of several message groups that VTAM issues in response to DISPLAY ID or DISPLAY TRL commands.
- As the first message in a message group that is issued when an IBM 10GbE RoCE Express interface or internal shared memory (ISM) interface becomes inoperative.
- As part of a message group that VTAM issues when it detects the failure of a Shared Memory Communications - Remote Direct Memory Access (SMC-R) link.
- As part of a message group that VTAM issues when it detects the failure of a Shared Memory Communications - Direct Memory Access (SMC-D) link.

When this message is issued in response to a DISPLAY command, this message is displayed for all TRLEs that are currently being used by at least one Upper-layer Protocol (ULP). A separate message IST1717I will be displayed for each ULP using this TRLE.

- For a dynamic TCP TRLE, or an exclusively owned TRLE, only one message with ULPID is issued, because there can only be one ULP using each of these TRLEs.
- For an OSA-Express Adapter, one message with ULPID is issued for each Datapath channel address in use by a ULP.
- For other TRLEs, more than one message with ULPID might be issued, depending on how many upper-layer protocols are using the TRLE.

When this message is issued in response to a 10GbE RoCE Express interface or ISM interface becoming inoperative, it is the first message in this message group:

```
IST1717I ULPID = ulp_id ULP INTERFACE = ulp_interface
IST1578I inoptype INOP DETECTED FOR trlename BY modname CODE = code
```

When this message is issued in response to an SMC-R link failure, this message is displayed to identify the TCP/IP stack associated with the failing SMC-R link. See message IST2406I for an explanation of the message group.

When this message is issued in response to an SMC-D link failure, this message is displayed to identify the TCP/IP stack associated with the failing SMC-D link. See message “IST2421I” on page 707 for an explanation of the message group.

IST1717I

This message provides ULP information.

ulp_id
Specifies the name of a z/OS Communications Server ULP that is using the TRLE, the SMC-R link, the SMC-D link, or one of the datapath channels of an OSA-Express TRLE.

- For TCP/IP ULPs, the *ulp_id* is the job name.
- For ANNC ULPs, the *ulp_id* is the SNA PU name.
- For ATM or EE ULPs, the *ulp_id* is the XCA major node name.

ulp_interface
Specifies the name of either the interface or the device that is using the TRLE, the SMC-R link, the SMC-D link, or one of the datapath channels of an OSA-Express TRLE.

- For TRLEs with MPCLEVEL=QDIO, *ulp_interface* is the name of the interface dedicated to this datapath channel address of the OSA-Express TRLE.
- For TRLEs with CONTROL=ROCE, *ulp_interface* is the name of the interface dedicated to the 10GbE RoCE Express TRLE.
- For TRLEs with CONTROL=ISM, *ulp_interface* is the name of the interface dedicated to the ISM TRLE.
- For all other TRLEs, *ulp_interface* is `*NA*`.
- For SMC-R links, *ulp_interface* is the name of the 10GbE RoCE Express interface that was being used by the failing link.
- For SMC-D links, *ulp_interface* is the name of the ISM interface that was being used by the failing link.

For detailed instructions about setting up an OSA-Express feature, see the zEnterprise System and System z10 OSA-Express Customer's Guide and Reference.

IST1578I

This message provides information about the inoperative condition for a 10GbE RoCE Express interface or ISM interface for the TCP/IP stack represented by *ulp_id*.

inoptype
Specifies the type of inoperative condition. In this message group, the only possible value is `DEVICE`.

trlename
Specifies the name of the system-generated TRLE that represents the 10GbE RoCE Express interface or ISM interface.

modname
Specifies the name of the module that detected the inoperative condition.

code
Identifies the point in *modname* where the inoperative condition was detected.

See message IST1578I for more details.

System action:

- When this message is issued in response to a DISPLAY command, processing continues.
- When this message is issued in response to a 10GbE RoCE Express interface or ISM interface becoming inoperative, the interface is deactivated. The TCP/IP stack might attempt recovery of the interface.
- When this message is issued in response to an SMC-R link failure, processing continues. See message IST2406I for more details.
- When this message is issued in response to an SMC-D link failure, processing continues. See message "IST2421I" on page 707 for more details

Operator response:

- When this message is issued in response to a DISPLAY command, none.
- When this message is issued in response to a 10GbE RoCE Express interface or ISM interface becoming inoperative, no further action is required. If recovery fails, save the system log for problem determination.

- When this message is issued in response to an SMC-R link or SMC-D link failure, contact the system programmer.

System programmer response:

- When this message is issued in response to a DISPLAY command, none.
- When this message is issued in response to a 10GbE RoCE Express interface or ISM interface becoming inoperative, use *code* to determine the correct course of action. See message IST1578I for more details.
- When this message is issued in response to an SMC-R link failure, use information in the IST2406I message group to determine the correct course of action. See message IST2406I for more details.
- When this message is issued in response to an SMC-D link failure, use information in the IST2421I message group to determine the correct course of action. See message "IST2421I" on page 707 for more details.

Routing code: 2

Descriptor code: 5

IST1865I GLOBAL INOPDUMP = *status*

Explanation: This message is the first in a group of messages in response to the DISPLAY INOPDUMP or MODIFY INOPDUMP commands. Possible message groups follow:

- In response to a DISPLAY INOPDUMP command when INOPDUMP is globally set for all control groups:

```
 IST350I DISPLAY TYPE = INOPDUMP
 IST1865I GLOBAL INOPDUMP = status
[IST924I  ---------------------------------]
[IST1954I TRL MAJOR NODE = trl_major_node_name]
[IST1866I TRLE = trlename INOPDUMP = ON]
⋮
 IST314I  END
```

- In response to a DISPLAY INOPDUMP command when INOPDUMP is selectively enabled for one or more control groups:

```
 IST350I DISPLAY TYPE = INOPDUMP
 IST1865I GLOBAL INOPDUMP = ON BY CONTROL GROUPS
 IST1904I INOPDUMP = current_value
[IST924I  ---------------------------------]
[IST1954I TRL MAJOR NODE = trl_major_node_name]
[IST1866I TRLE = trlename INOPDUMP = ON]
⋮
 IST314I  END
```

- In response to a MODIFY INOPDUMP command:

```
 IST1865I GLOBAL INOPDUMP = status
[IST1866I TRLE = trlename INOPDUMP = status]
⋮
[IST1867I INOPDUMP = status FOR ALL TRLE BASED RESOURCES]
 IST223I MODIFY COMMAND COMPLETE
 IST314I  END
```

- In response to a MODIFY VTAMOPTS, INOPDUMP command:

```
IST1865I GLOBAL INOPDUMP = status
IST1867I INOPDUMP = status FOR ALL TRLE BASED RESOURCES
IST314I  END
```

IST223I

VTAM issues this message when the MODIFY command has successfully completed.

IST350I

This message identifies the type of information shown in the display. For this message group, type is always INOPDUMP.

IST1865I

- *status* can be one of the following:

- ON indicates that all active non-TRLE controlled resources might attempt to initiate an automatic VTAM dump when an inoperative condition is detected.
- OFF indicates that no active non-TRLE controlled resources will attempt to initiate an automatic VTAM dump when an inoperative condition is detected.
- ON BY CONTROL GROUPS indicates that INOPDUMP has been selectively enabled for resources identified by specific control group classifications. These resources might attempt to initiate an automatic VTAM dump when an inoperative condition is detected.
- OFF BY CONTROL GROUPS indicates that INOPDUMP has been selectively disabled for resources identified by specific control group classifications. These resources will not attempt to initiate an automatic VTAM dump when an inoperative condition is detected.

- The global INOPDUMP status is the default used to initialize each TRLE-based resource INOPDUMP status when the TRLEs are activated.

IST1866I

- If you receive this message in response to a DISPLAY INOPDUMP command, it will appear once for each TRLE with INOPDUMP=ON.
- *trlename* is the name of the TRLE for which status is being reported.
- *status* can be one of the following:
  - ON indicates that the resources defined in the TRLE might attempt to initiate an automatic VTAM dump when an inoperative condition is detected.
  - OFF indicates that the resources defined in the TRLE will not attempt to initiate an automatic VTAM dump when an inoperative condition is detected.

IST1867I

- *status* can be one of the following:
  - ON indicates that the INOPDUMP status for every TRLE in all active predefined TRL major nodes has been set to ON.
  - OFF indicates that the INOPDUMP status for every TRLE in all active predefined TRL major nodes has been set OFF.
  - SELECTIVELY PROCESSED indicates that a MODIFY VTAMOPTS,INOPDUMP command has been issued to enable or disable INOPDUMP processing selectively by control groups. The INOPDUMP status for every TRLE in all active predefined TRL major nodes which match the specified control groups has been set appropriately.
- This message is a reminder to the operator that use of the MODIFY VTAMOPTS,INOPDUMP command or a global MODIFY INOPDUMP command also sets the INOPDUMP status for each TRLE in all active predefined TRL major nodes. However, if there are no active predefined TRL major nodes, this message will not appear in the response.

IST1904I

INOPDUMP is the name of the VTAM start option.

current_value lists the names of the INOPDUMP control groups which are currently enabled. See the z/OS Communications Server: SNA Resource Definition Reference for more information regarding INOPDUMP control groups.

IST1954I

trl_major_node_name is the name of the TRL major node defining the TRLE for which status is being reported.

This message is issued once for each active predefined TRL major node.

System action: Processing continues

Operator response: None.

System programmer response: None.

Routing code: 2

Descriptor code: 5

IST1904I *option* **=** *current_value*

Explanation: VTAM issues this message as part of a group of messages in response to a DISPLAY VTAMOPTS or DISPLAY INOPDUMP command. The first message in these groups are IST1188I and IST1865I, respectively. See the explanation of those messages for a complete description.

Routing code: 2

Descriptor code: 5

IST2337I **CHPID TYPE =** *chpid_type* **CHPID =** *chpid_num* **PNETID =** *net_id*

Explanation: This message is part of several message groups that VTAM issues in response to a DISPLAY ID or DISPLAY TRL command. See "IST1221I" on page 684 for a complete description.

VTAM also issues this message as part of a group of messages that the adapter interrupt monitoring function generates. The first message in the group is IST2419I. See "IST2419I" on page 705 for a complete description.

Routing code: 2

Descriptor code: 5

IST2390I **IQP1REG PCIE SERVICE FAILURE**

Explanation: This is the first message in a message group that VTAM issues when an attempt to register a Peripheral Component Interconnect Express (PCIe) device fails. VTAM uses PCIe services as part of managing PCIe devices, and part of that management is registering the devices. VTAM uses PCIe services to manage these devices:

- IBM 10GbE RoCE Express interfaces
- Internal shared memory (ISM) interfaces

A complete description of the message group follows:

```
IST2390I IQP1REG PCIE SERVICE FAILURE
IST1684I RETURN CODE = return_code REASON CODE = reason_code
IST314I END
```

IST1684I

This message provides the specific return code and reason code information that the failing PCIe service returns.

In the message text:

return_code
The hexadecimal return code that the PCIe IQP1REG invocation returns.

reason_code
The hexadecimal reason code that the PCIe IQP1REG invocation returns.

IST2390I

This message is the first message in the message group.

System action: Processing continues. VTAM will again attempt to register the PCIe devices the next time a TCP/IP stack issues an activation request for a 10GbE RoCE Express interface or an ISM interface.

Operator response: Contact the system programmer.

System programmer response: Collect VTAM internal traces at the VTAM that issued this message and contact IBM service to determine the reason for the registration failure.

User response: Not applicable.

Problem determination: None.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f*

procname,msgmod=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is a candidate for automation to detect errors that occur during activation of PCIe devices.

Example:

```
IST2390I IQP1REG PCIE SERVICE FAILURE
IST1684I RETURN CODE = 18 REASON CODE = 5035
IST314I END
```

IST2391I *service_name* **PCIE SERVICE FAILURE ON TRLE** *trle_name*

Explanation: This is the first message in a message group that VTAM issues when an attempt to use a Peripheral Component Interconnect Express (PCIe) service fails. VTAM uses PCIe services to manage these devices:

- IBM 10GbE RoCE Express interfaces
- Internal shared memory (ISM) interfaces

A complete description of the message group follows:

```
IST2391I service_name PCIE SERVICE FAILURE ON TRLE trlename
IST1684I RETURN CODE = return_code REASON CODE = reason_code
IST314I END
```

IST1684I

This message provides the specific return code and reason code information that the failing PCIe service returns.

In the message text:

return_code
The hexadecimal return code that the PCIe *service_name* invocation returns.

reason_code
The hexadecimal reason code that the PCIe *service_name* invocation returns.

IST2391I

This message identifies the PCIe service that failed.

In the message text:

service_name
The PCIe service that failed.

trle_name
The name of the associated transport resource list entry (TRLE) that VTAM was managing when the PCIe service failed. The TRLE name represents an individual 10GbE RoCE Express port or ISM device. VTAM automatically generates the TRLE name when the TCP/IP stack starts the interface.

System action: Processing continues.

Operator response: Contact the system programmer.

System programmer response: Collect VTAM internal traces at the VTAM that is issuing this message and contact IBM service to determine the reason for the PCIe service failure.

User response: Not applicable.

Problem determination: None.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is a candidate for automation to detect errors that occur during activation of PCIe devices.

Example:

```
IST2391I IQP4ALL PCIE SERVICE FAILURE ON TRLE IUT10018
IST1684I RETURN CODE = 18 REASON CODE = 5035
IST314I END
```

IST2392I PFID *pfid_value* ALLOCATION FAILURE - PFID IS NOT DEFINED

Explanation: VTAM issues this message when it attempts to activate a Peripheral Component Interconnect Express (PCIe) device, but the PCIe function ID (PFID) value is not defined for this LPAR. VTAM uses PCIe services to manage these devices:

- IBM 10GbE RoCE Express interfaces
- Internal shared memory (ISM) interfaces

In the message text:

pfid_value
The PFID value that VTAM used in the failed activation attempt.

System action: Processing continues.

Operator response: Issue the **D PCIE** command and generate a Netstat CONFIG/-f report, and then provide the output to the system programmer.

System programmer response:

1. Determine the correct PFID value for this system.
2. Use the **D PCIE** command output to verify that the PFID value has been correctly defined in the HCD. If the PFID is not defined properly, update the HCD configuration to include the correct PFID value.
3. If the PFID is defined correctly in the HCD and represents a 10GbE RoCE Express interface, use the Netstat CONFIG/-f report to verify that the correct PFID is defined to TCP/IP. If the PFID is not defined correctly, change the SMCR parameter on the GLOBALCONFIG statement in the TCP/IP profile of the TCP/IP stack that is attempting to activate this 10GbE RoCE Express interface to specify the correct PFID value.
4. If the PFID is defined correctly in the HCD and represents an ISM interface, then verify that the physical network ID (PNetID) attributes of the PFID and the corresponding OSD or HiperSockets interfaces match in the HCD. If they do not match, correct the definitions so that the proper PNetID is used.
5. Instruct the operator to issue the necessary commands to activate the changes that were made to the HCD or the TCP/IP profile.

User response: Not applicable.

Problem determination: None.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is a candidate for automation to detect errors that occur during activation of PCIe devices.

Example:

```
IST2392I PFID 0018 ALLOCATION FAILURE - PFID IS NOT DEFINED
```

IST2393I PFID *pfid_value* **ALLOCATION FAILURE - PFID IS NOT ONLINE**

Explanation: VTAM issues this message when it attempts to activate a Peripheral Component Interconnect Express (PCIe) device using the correct PCIe function ID (PFID) value, but the device that is associated with that PFID is not online. VTAM uses PCIe services to manage these devices:

- IBM 10GbE RoCE Express interfaces
- Internal shared memory (ISM) interfaces

In the message text:

pfid_value
The PFID value that VTAM used in the failed activation attempt.

System action: Processing continues.

Operator response:

1. Issue the **CF PFID** command to bring the PCIe device that is associated with the *pfid_value* online.
2. Issue the **VARY START** command to start the 10GbE RoCE Express or ISM interface.

System programmer response: None.

User response: Not applicable.

Problem determination: None.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is a candidate for automation to detect errors that occur during initialization of your system.

Example:

```
IST2393I PFID 0018 ALLOCATION FAILURE - PFID IS NOT ONLINE
```

IST2407I LOCAL LINK ID = *local_id* **REMOTE LINK ID =** *remote_id*

Explanation: VTAM issues this message as part of a group of messages when a Shared Memory Communications - Remote Direct Memory Access (SMC-R) link or Shared Memory Communications - Direct Memory Access (SMC-D) link failure is detected. VTAM issues message group IST2406I for SMC-R link failures and message group IST2421I for SMC-D link failures. See message IST2406I or "IST2421I" on page 707 for an explanation of the message group.

System action: See message group for details.

Operator response: See message group for details.

System programmer response: See message group for details.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is not a candidate for automation.

Example:

```
IST2407I LOCAL LINK ID = 2D8F0100  REMOTE LINK ID = 729D0101
```

IST2409I *type* **GID =** *gid_value*

Explanation: VTAM issues this message as part of a group of messages when a Shared Memory Communications - Remote Direct Memory Access (SMC-R) link or Shared Memory Communications - Direct Memory Access (SMC-D) link failure is detected. VTAM issues message group IST2406I for SMC-R link failures and message group IST2421I for SMC-D link failures. See message IST2406I or "IST2421I" on page 707 for an explanation of the message group.

System action: See message group for details.

Operator response: See message group for details.

System programmer response: See message group for details.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is not a candidate for automation.

Example:

```
IST2409I LOCAL GID = FE80::200:1FF:FE12:F030
```

IST2411I **VLAN =** *vlan_id*

Explanation: VTAM issues this message as part of a group of messages when a Shared Memory Communications - Remote Direct Memory Access (SMC-R) link or Shared Memory Communications - Direct Memory Access (SMC-D) link failure is detected. VTAM issues message group IST2406I for SMC-R link failures and message group IST2421I for SMC-D link failures. See message IST2406I or "IST2421I" on page 707 for an explanation of the message group.

System action: See message group for details.

Operator response: See message group for details.

System programmer response: See message group for details.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is not a candidate for automation.

Example:

```
IST2411I VLAN = 100
```

IST2417I VFN = *virtual_function_number*

Explanation: VTAM issues this message as part of several message groups in response to a DISPLAY ID or DISPLAY TRL command.

See message IST2361I for an explanation of the message group when the TRLE represents an IBM 10GbE RoCE Express interface, or message IST2418I when the TRLE represents an internal shared memory (ISM) interface.

System action: Processing continues.

Operator response: None.

System programmer response: None.

User response: None.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is not a candidate for automation.

Example:

```
IST2417I VFN = 0002
```

IST2418I SMCD PFID = *pfid* **VCHID =** *vchid* **PNETID =** *network_id*

Explanation: VTAM issues this message as part of a message group in response to a DISPLAY ID or DISPLAY TRL command for a TRLE that is associated with an internal shared memory (ISM) device.

VTAM also issues this message as part of a group of messages that the adapter interrupt monitoring function generates. The first message in the group is IST2419I. See "IST2419I" on page 705 for a complete description.

A complete description of the message group follows the example:

```
IST075I NAME = nodename, TYPE = nodetype
IST1954I TRL MAJOR NODE = trl_major_node_name
IST486I STATUS= current_status, DESIRED STATE= desired_state
IST087I TYPE = line_type, CONTROL = line_control, HPDT = hpdtvalue
IST2418I SMCD PFID = pfid  VCHID = vchid  PNETID = network_id
IST2417I VFN = virtual_function_number
[IST924I ------------------------------------------]
[IST1717I ULPID = ulp_id ULP INTERFACE = ulp_interface]
[IST1724I I/O TRACE = iotrc TRACE LENGTH = length]
```

IST075I

This message displays the resource name and resource type.

nodename
The name of the resource that was entered on the DISPLAY command.

nodetype
The resource type of the major or minor node. The *nodetype* value is always **TRLE** for this message group.

IST087I

IST2418I

This message displays line information associated with *nodename*.

line_type
The *line_type* value is always ***NA*** for this message group.

line_control
The *line_control* value is always **ISM** (internal shared memory) for this message group.

hpdtvalue
The *hpdtvalue* value is always ***NA*** for this message group.

IST486I

This message displays status information for *nodename*.

current_status
The current status of the node. See the z/OS Communications Server: IP and SNA Codes for status information.

desired_state
The node state that is desired. See the z/OS Communications Server: IP and SNA Codes for status information. If VTAM cannot determine the desired state, *desired_state* is ***NA***.

IST1717I

This message is displayed when the ISM TRLE is currently being used by a upper-layer protocol (ULP). Only one ULP can use an ISM TRLE at a time.

ulp_id The name of a z/OS Communications Server ULP that is using the ISM TRLE. In this message group, the *ulp_id* value is always the TCP/IP job name.

ulp_interface
The name of the interface associated with the ISM TRLE.

IST1724I

This message displays trace information for *nodename*.

iotrc Specifies whether I/O Trace is active for *nodename*. In this message group, the *iotrc* value is always **OFF**.

length Specifies the number of bytes being recorded for I/O Trace for *nodename*. In this message group, the *length* value is always ***NA***.

IST1954I

This message displays the TRL major node name.

trl_major_node_name
The name of the TRL major node defining the ISM TRLE. The *trl_major_node_name* value is always ISTTRL for this message group.

IST2417I

This message displays the virtual function number (VFN) associated with *nodename*.

virtual_function_number
The virtual function number.

IST2418I

This message provides configuration information for the ISM device represented by *nodename*.

pfid The 2-byte hexadecimal Peripheral Component Interconnect Express (PCIe) function ID.

vchid The 2-byte hexadecimal virtual channel ID (VCHID).

network_id
The physical network identifier.

System action: Processing continues.

Operator response: Not applicable.

System programmer response: Not applicable.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is not a good candidate for automation.

Example:

```
IST097I DISPLAY ACCEPTED
IST075I NAME = IUT0001D, TYPE = TRLE
IST1954I TRL MAJOR NODE = ISTTRL
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = *NA*, CONTROL = ISM, HPDT = *NA*
IST2418I SMCD PFID = 001D  VCHID = 0178  PNETID = NETWORK1
IST2417I VFN = 0002
IST924I -------------------------------------------------------------
IST1717I ULPID = TCPCS ULP INTERFACE = EZAISM03
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST314I END
```

IST2419I VIRTUAL INTERRUPT DRIVEN FOR TRLE *trlename*

Explanation: VTAM issues this message as part of a group of messages generated by the adapter interrupt monitoring function. This message group indicates VTAM detected that no interrupt had been generated for the interface associated with *trlename* even though there was data waiting to be processed, and that VTAM then initiated a virtual interrupt to resume activity on the interface. The adapter interrupt monitoring function is enabled using the AIMON start option.

A complete description of the message group follows the example:

```
IST2419I VIRTUAL INTERRUPT DRIVEN FOR TRLE trlename
[ IST2337I CHPID TYPE = chpid_type CHPID = chpid_num PNETID = network_id]
[ IST2361I SMCR PFID = pfid PCHID = pchid PNETID = network_id ]
[ IST2418I SMCD PFID = pfid VCHID = vchid PNETID = network_id ]
IST314I END
```

IST2337I

This message provides configuration information for the OSA-Express adapter that is associated with *trlename*.

chpid_type
The type of channel path identifier that this TRLE uses:

OSD Channel type for an OSA-Express CHPID that is configured in QDIO mode.

OSM Channel type for an OSA-Express CHPID that is configured for attachment to the intranode management network.

OSX Channel type for an OSA-Express CHPID that is configured for attachment to the intraensemble network.

chpid_mum
The 2-byte hexadecimal virtual channel path identifier (CHPID) for the OSA-Express adapter.

network_id
The physical network identifier for the OSA-Express adapter that is associated with *trlename*.

IST2361I

This message provides configuration information for the adapter associated with *trlename*.

pfid The 2-byte hexadecimal Peripheral Component Interconnect Express (PCIe) function ID for the 10GbE RoCE Express feature associated with *trlename*.

pchid The 2-byte hexadecimal physical channel ID (PCHID) for the 10GbE RoCE Express feature associated with *trlename*.

network_id
The physical network identifier for the 10GbE RoCE Express interface associated with *trlename*.

IST2418I

This message provides configuration information for the device that is associated with *trlename*.

pfid The 2-byte hexadecimal Peripheral Component Interconnect Express (PCIe) function ID for the internal shared memory (ISM) device that is associated with *trlename*.

vchid The 2-byte hexadecimal virtual channel ID (VCHID) for ISM device that is associated with *trlename*.

network_id
The physical network identifier for the ISM interface that is associated with *trlename*.

IST2419I

This is the first message in the message group.

trlename
The name of the resource for which VTAM drove a virtual interrupt.

System action: Processing continues.

Operator response: Contact the system programmer.

System programmer response: If this error occurs repeatedly, instruct the operator to issue this command:

MODIFY CSDUMP,MESSAGE=IST2419I

Issue this command to collect a VTAM dump the next time this message group is displayed. When the diagnostic information is collected, contact IBM Service.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is not a good candidate for automation.

Example:

```
IST2419I VIRTUAL INTERRUPT DRIVEN FOR TRLE IUT10010
IST2361I SMCR PFID = 0010  PCHID = 01A0  PNETID = NETID1
IST314I END
```

IST2420I ISM NOT SUPPORTED, REQUIRED HARDWARE NOT AVAILABLE

Explanation: VTAM issues this message when it detects that internal shared memory (ISM) processing cannot be performed because the necessary hardware is not available. VTAM uses ISM processing as part of Shared Memory Communications - Direct Memory Access (SMC-D) processing.

System action: Processing continues. Future attempts to activate the ISM device will fail.

Operator response: Contact the system programmer.

System programmer response: Ensure that the TCP/IP stack configured to use SMC-D processing is operating on an IBM z13 GA2/MR or later processor.

You can configure a TCP/IP stack to use SMC-D by specifying the SMCD parameter on the GLOBALCONFIG statement.

If you cannot operate the TCP/IP stack on an IBM z13 GA2/MR or later processor, make one of the following changes to the GLOBALCONFIG statement for the TCP/IP stack:

- Remove the SMCD operand.
- Specify the NOSMCD operand.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is a candidate for automation to detect errors that occur during activation of PCIe devices.

Example:

```
IST2420I ISM NOT SUPPORTED, REQUIRED HARDWARE NOT AVAILABLE
```

IST2421I SMC-D LINK FAILURE ON TRLE trlename CODE = rsn_code

Explanation: VTAM issues this group of messages when a Shared Memory Communications - Direct Memory Access (SMC-D) link failure is detected.

A complete description of the message group follows:

```
IST2421I SMC-D LINK FAILURE ON TRLE trlename CODE = rsn_code
IST1717I ULPID = ulp_id ULP INTERFACE = ulp_interface
IST2407I LOCAL LINK ID = local_id REMOTE LINK ID = remote_id
IST2409I type GID = gid_value
[IST2411I VLAN = vlan_id]
IST314I END
```

IST1717I

This message is displayed to identify the upper-layer protocol (ULP) associated with the failing SMC-D link.

ulp_id The name of a z/OS Communications Server ULP. In this message group, the *ulp_id* value is always the TCP/IP job name.

ulp_interface
The name of the internal shared memory (ISM) interface that was used by the failing SMC-D link.

IST2407I

IST2421I

This message displays the SMC-D link identification values assigned to the failing SMC-D link.

local_id The SMC-D link ID value assigned by this node for the failing SMC-D link.

remote_id
The SMC-D link ID value assigned by the remote SMC-D peer for the failing SMC-D link.

IST2409I

This message displays a group ID (GID) value for the failing SMC-D link.

type Indicates which SMC-D link peer generated this GID value. Possible values are:

LOCAL
The GID value was assigned by this node.

REMOTE
The GID value was assigned by the remote SMC-D peer.

gid_value
The GID value assigned by the SMC-D peer for the failing SMC-D link.

IST2411I

This optional message is displayed when a virtual LAN (VLAN) is associated with the failing SMC-D link.

vlan_id The VLAN value associated with the failing SMC-D link.

IST2421I

This is the first message in the message group.

trlename
The name of the TRLE that represents the ISM interface that was used by the failing SMC-D link.

rsn_code
The reason code generated by z/OS Communications Server to assist in identifying the reason for the SMC-D link failure.

System action: Processing continues. The TCP connections that are using the failing SMC-D link end.

Operator response: Contact the system programmer.

System programmer response: For more information about Data Link Control (DLC) status codes and about the error that the value of *rsn_code* reports, see z/OS Communications Server: IP and SNA Codes. Perform the necessary corrections, if any.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is not a good candidate for automation.

Example:

```
IST2421I SMC-D LINK FAILURE ON TRLE IUT00018 CODE = 80145701
IST1717I ULPID = TCPCS1 ULP INTERFACE = EZAISM01
IST2407I LOCAL LINK ID = 00010000 REMOTE LINK ID = 00000000
```

```
IST2409I LOCAL GID = 8002000A000A0061
IST2409I REMOTE GID = 8002000A000A0062
IST2411I VLAN = 100
IST314I END
```

IST2422I NO ISM PFIDS DEFINED FOR PNETID *pnetid_value*

Explanation: VTAM issues this message when it attempts to activate an internal shared memory (ISM) device associated with a physical network ID (PNetID), but no Peripheral Component Interconnect Express (PCIe) function ID (PFID) values are defined for this PNetID.

In the message text:

pnetid_value
The physical network ID that VTAM used in the failed activation attempt.

System action: ISM interface activation fails.

Operator response: Issue the D PCIE command and provide the output to the system programmer.

System programmer response: Determine if *pnetid_value* is a valid physical network ID for this system, and perform one of the following steps:

- If the *pnetid_value* is not valid, correct the OSD or HiperSockets definitions in the HCD. VTAM learns the PNetID of the OSD and Hipersockets devices during activation processing. These PNetID values are subsequently used to attempt to activate internal shared memory (ISM) interfaces associated with Shared Memory Communications - Direct Memory Access (SMC-D) capable OSD or HiperSockets devices.
- If the *pnetid_value* is valid, correct the HCD definitions for the PFID values that should be used for *pnetid_value* interfaces.

After the corrections have been made, instruct the operator to issue the necessary commands to activate the changes that were made to the HCD configuration.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is a candidate for automation to detect errors that occur during activation of ISM devices.

Example:

```
IST2422I NO ISM PFIDS DEFINED FOR PNETID NETID2
```

IST2423I NO ISM PFIDS AVAILABLE FOR PNETID *pnetid_value*

Explanation: VTAM issues this message when it attempts to activate an internal shared memory (ISM) interface associated with a physical network ID (PNetID). Peripheral Component Interconnect Express (PCIe) function ID (PFID) values are defined for this PNetID, but none of the PCIe devices associated with the PFID values are available.

In the message text:

pnetid_value
The physical network ID that VTAM used in the failed activation attempt.

System action: ISM interface activation fails.

Operator response: Take the following steps to correct the problem:

1. Issue the D PCIE command to identify the PFID values that are associated with *pnetid_value*.
2. If any PCIe devices associated with *pnetid_value* are offline, take the following steps:
   - Issue the CF PFID command to bring the PCIe devices associated with the PFID values online.
   - Issue the VARY START command to start the internal shared memory (ISM) interface.
3. If all PCIe devices associated with *pnetid_value* are online, contact the system programmer.

System programmer response: If all PCIe devices associated with *pnetid_value* are online and in use, and you want additional TCP/IP stacks to activate ISM interfaces for this *pnetid_value*, take the following steps:

1. Update the HCD configuration to define additional virtual functions (VF) for the virtual channel ID (VCHID) representing the ISM device used by *pnetid_value*.
2. After the corrections have been made, instruct the operator to issue the necessary commands to activate the changes that were made to the HCD configuration and to issue the VARY START command to start the ISM interface.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: This message is a candidate for automation to detect errors that occur during activation of ISM devices.

Example:

```
IST2423I NO ISM PFIDS AVAILABLE FOR PNETID NETID2
```

Chapter 16. Summary of Message and Interface Changes

Communications Server IP summary of interface changes

This topic describes the updates to the following Communications Server IP interfaces:

- PROFILE.TCPIP configuration file
  - "PROFILE.TCPIP statement and parameter changes" on page 712
- Configuration Files (other than PROFILE.TCPIP)
  - FTP client configuration statements
  - FTP server configuration statements
  - TN3270E Telnet server PROFILE configuration file
    - BEGINVTAM information block
    - TELNETGLOBALS information block
    - TELNETPARMS information block
  - General updates for the non-PROFILE.TCPIP IP configuration files
- RACF interfaces
- Operator commands
  - "Netstat operator commands (DISPLAY TCPIP,,NETSTAT)" on page 720
  - TN3270E Telnet server operator commands
  - "General updates of IP operator commands" on page 729
- TSO commands
  - "NETSTAT TSO commands" on page 733
  - FTP TSO and z/OS UNIX commands
    - FTP subcommands
  - General updates of TSO commands
- z/OS UNIX commands
  - "Netstat UNIX commands" on page 739
  - General updates of z/OS UNIX commands
- Application programming interfaces and network management interfaces
  - FTP client API FCAI control block
  - FTP client API for REXX predefined variables
  - Local IPSec NMI
  - Network security services NMI
  - Real-time application-controlled TCP/IP trace NMI (EZBRCIFR)
  - Real-time network monitoring TCP/IP NMI
  - Resolver callable NMI (EZBREIFR)
  - SNMP manager API
  - Syslog daemon name/token pair
  - "TCP/IP callable NMI (EZBNMIFR)" on page 746
  - Trace formatting NMI (EZBCTAPI)
  - Trusted TCP connections API for Java
- Environment variables
- Socket APIs
  - General updates of socket APIs
- IPCS subcommands
  - CTRACE COMP(SYSTCPDA) subcommand
  - CTRACE COMP(SYSTCPIS) subcommand
  - CTRACE COMP(SYSTCPOT) subcommand
  - CTRACE COMP(SYSTCPRE) subcommand
  - "TCPIPCS subcommand" on page 759
  - General updates to IPCS subcommands
- SNMP MIB modules

- INITDB start option
- Application data
- FTP client error codes
- SMF record type 119 enhancements
  - CSSMTP records
  - FTP records
  - IPSec records
  - SMC-R records
  - TCP connection records
  - "TCP/IP stack records" on page 761
  - TN3270E Telnet server records
- General updates of IP interfaces
- Samples provided in MVS data set SEZAINST
- Samples provided in z/OS UNIX TCPIP directory

PROFILE.TCPIP statement and parameter changes

Table 23 lists the new and updated Communications Server PROFILE.TCPIP configuration statements and parameters. See *z/OS Communications Server: IP Configuration Reference* for more detailed information.

Table 23. Summary of new and changed Communications Server PROFILE.TCPIP configuration statements and parameters

Statement	Release	Description	Reason for change
ATMARPSV, ATMLIS, ATMPVC	V2R2	Support for these profile statements is removed because the ATM device type is no longer supported.	Removed support for legacy devices
	V2R1	Because support for the ATM device type will be dropped in a future release, these profile statements will no longer be supported then.	IBM Health Checker for legacy device types
AUTOLOG	V2R1	Message EZZ0621I or EZZ0622I will be issued on the first cancel of an autologged procedure.	Release update
DELETE PORT DELETE PORTRANGE	V2R1	For TCP ports, if no reservation is found for the port or the reservation was deleted in the current profile processing, error message EZZ0328I is issued instead of message EZZ0395I. Message EZZ0395I will continue to be issued for other errors. Update your message automation for this change.	Release update
DEVICE	V2R2	The following DEVICE types and their corresponding LINK profile statements are no longer supported: • ATM • CDLC • CLAW • HYPERchannel • SNALINK (LU0 and LU6.2) • X.25	Removed support for legacy devices

Table 23. Summary of new and changed Communications Server PROFILE.TCPIP configuration statements and parameters (continued)

Statement	Release	Description	Reason for change
DEVICE and LINK	V2R2	Support for the DEVICE and LINK profile statements for the following TCP/IP legacy device types will be dropped in a future release: • FDDI and Token Ring (LCS with LINKs FDDI and IBMTR) • Token Ring (MPCIPA with LINK IPAQTR) • Ethernet and FDDI (MPCOSA with LINKs OSAENET and OSAFDDI)	IBM Health Checker for additional z/OS legacy device types
	V2R1	Support for the DEVICE and LINK profile statements for the following TCP/IP legacy device types will be dropped in a future release: • ATM • CDLC • CLAW • HYPERchannel • SNALINK (LU0 and LU6.2) • X.25	IBM Health Checker for legacy device types
GATEWAY	V2R2	Support for this profile statement is removed. The BEGINROUTES statement can be used to configure static routes.	Removed support for the GATEWAY statement in the TCP/IP profile
	V2R1	Support for this profile statement will be dropped in a future release. Use the BEGINROUTES/ENDROUTES configuration block to replace your GATEWAY statements. To assist in converting your GATEWAY statements to BEGINROUTES statements, you can take a dump of the TCP/IP stack address space and use the CONVERT parameter on the IPCS TCPIPCS PROFILE subcommand. The TCPIPCS command output will contain the information that is specified on the GATEWAY statements converted to the equivalent BEGINROUTES/ENDROUTES statements. See "TCPIPCS PROFILE" in the IP Diagnosis Guide for more information.	IBM Health Checker for z/OS GATEWAY statement check

Table 23. Summary of new and changed Communications Server PROFILE.TCPIP configuration statements and parameters (continued)

Statement	Release	Description	Reason for change
GLOBALCONFIG	V2R2	The SMCD parameter is defined to enable and configure the Shared Memory Communications - Direct Memory Access (SMC-D) function. The SMCD parameter includes the FIXEDMEMORY and TCPKEEPMININTERVAL subparameters. The NOSMCD parameter is defined to disable SMC-D function.	Shared Memory Communications - Direct Memory Access
	V2R2	The ADJUSTDVIPAMSS parameter is added to control whether TCP/IP adjusts the Maximum Segment Size for TCP connections.	VIPAROUTE fragmentation avoidance
	V2R2	For the SMCR parameter, a new value of 4096 can be specified for the MTU subparameter.	Shared Memory Communications over RDMA enhancements
	V2R2	Added SMCGLOBAL parameter to provide global settings for the Shared Memory Communications over Remote Direct Memory Access (SMC-R) function and Shared Memory Communications - Direct Memory Access (SMC-D) function. The following subparameters can be specified: • AUTOCACHE and NOAUTCACHE Control caching of unsuccessful attempts to use SMC-R or SMC-D. • AUTOSMC and NOAUTOSMC Control monitoring incoming TCP connections to determine whether they would benefit from SMC-R or SMC-D.	• Shared Memory Communications over RDMA enhancements • Shared Memory Communications - Direct Memory Access (SMC-D)
	V2R1	The PFID operand on the SMCR statement is changed to accept a range of values between X'0000' and X'0FFF'.	Shared Memory Communications over RDMA adapter (RoCE) virtualization
	V2R1	The SMCR parameter is defined to enable and configure Shared Memory Communications over Remote Direct Memory Access (SMC-R) function. The SMCR parameter includes the PFID, PORTNUM, MTU, FIXEDMEMORY, and TCPKEEPMININTERVAL sub-parameters. The NOSMCR parameter is defined to disable SMC-R function.	Shared Memory Communications over Remote Direct Memory Access
GLOBALCONFIG	V1R13	Deprecated the SEGMENTATIONOFFLOAD and NOSEGMENTATIONOFFLOAD parameters.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	V1R13	Added the AUTOIQDX and NOAUTOIQDX parameters. The AUTOIQDX parameter includes the ALLTRAFFIC and NOLARGEDATA sub-parameters.	HiperSockets optimization for intraensemble data networks

Table 23. Summary of new and changed Communications Server PROFILE.TCPIP configuration statements and parameters (continued)

Statement	Release	Description	Reason for change
INTERFACE	V2R2	The SMCD parameter is defined to enable the SMC-D function for the following statements: • IPAQENET, when CHPIDTYPE OSD is specified • IPAQENET6, when CHPIDTYPE OSD is specified • IPAQIDIO • IPAQIDIO6 The NOSMCD parameter is defined to disable the SMC-D function.	Shared Memory Communications - Direct Memory Access
	V2R1	Can be used to configure IPv4 HiperSockets interfaces (IPAQIDIO) instead of the DEVICE, LINK, and HOME statements.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	V2R1	Can be used to configure IPv4 static VIPA interfaces (VIRTUAL) instead of the DEVICE, LINK, and HOME statements.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	V2R1	For IPAQENET interface types, added new TEMPIP parameter to allow an interface to activate without an IP address assigned. Applications which implement DHCP client support can communicate over the interface to obtain an IP address.	Enable DHCP clients on OSA Interfaces
	V2R1	The SMCR parameter is defined to enable Shared Memory Communications - RDMA (SMC-R) function for IPAQENET and IPAQENET6 statements. The SMCR parameter is valid only for CHPIDTYPE OSD definitions. The NOSMCR parameter is defined to disable SMC-R function.	Shared Memory Communications over Remote Direct Memory Access
IPCONFIG	V2R2	The SMCD subparameter is defined on this statement for the DYNAMICXCF parameter to enable the SMC-D function. The NOSMCD subparameter is defined to disable SMC-D function.	Shared Memory Communications - Direct Memory Access
	V2R2	Support for the CLAWUSEDOUBLENOP and STOPONCLAWERROR parameters is removed because the CLAW device type is no longer supported.	Removed support for legacy devices
	V2R1	You can enable QDIOACCELERATOR when IPSECURITY is enabled.	QDIO acceleration coexistence with IP filtering
	V2R1	The SOURCEVIPAINTERFACE parameter is added for IPv4 DYNAMICXCF interfaces.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	V1R13	Added CHECKSUMOFFLOAD and NOCHECKSUMOFFLOAD and SEGMENTATIONOFFLOAD and NOSEGMENTATIONOFFLOAD parameters.	OSA-Express4S QDIO IPv6 checksum and segmentation offload

Table 23. Summary of new and changed Communications Server PROFILE.TCPIP configuration statements and parameters (continued)

Statement	Release	Description	Reason for change
IPCONFIG6	V2R2	The SMCD subparameter is defined on this statement for the DYNAMICXCF parameter to enable the SMC-D function. The NOSMCD subparameter is defined to disable SMC-D function.	Shared Memory Communications - Direct Memory Access
	V1R13	Added CHECKSUMOFFLOAD and NOCHECKSUMOFFLOAD and SEGMENTATIONOFFLOAD and NOSEGMENTATIONOFFLOAD parameters.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	V1R13	If you do not specify the IGNOREREDIRECT parameter and you are using Intrusion Detection Services (IDS) policy to detect and discard Redirect packets, ICMPv6 Redirect packets are discarded while the policy is active.	Expanded Intrusion Detection Services
IPSEC	V2R2	The IPSECRULE and IPSEC6RULE statements support new and modified parameters that can be used to configure enhanced default IP filter policy.	TCPIP profile IP security filter enhancements
	V2R2	A new parameter, DVLOCALFLTR, is added to the IPSEC statement. DVLOCALFLTR enables IP filtering of TCP traffic between a client and an IPv4 dynamic VIPA defined on the same TCP/IP stack, when the traffic is forwarded to another TCP/IP stack.	APAR PI44865
	V2R1		APAR PI40291
	V2R1	The DVIPSEC parameter enables the support for Sysplex-Wide Security Associations (SWSA) for IPv6 on a stack that also has the IPSECURITY parameter specified on the IPCONFIG6 statement.	Sysplex-Wide Security Associations for IPv6
NETACCESS	V2R1	The CACHEALL, CACHEPERMIT, and CACHESAME parameters are added to control the level of caching that is used for the results of network access control checks.	Improve auditing of NetAccess rules
NETMONITOR	V2R1	The PROFILE and NOPROFILE subparameters control the creation of both the TCP/IP stack SMF 119 profile record (subtype 4) and the new TN3270E Telnet server SMF 119 profile record (subtype 24).	NMI and SMF enhancements for TCP/IP applications

Table 23. Summary of new and changed Communications Server PROFILE.TCPIP configuration statements and parameters (continued)

Statement	Release	Description	Reason for change
PORT	V2R2	• The SMC parameter is enhanced to enable SMC-D function for the specified port. • The NOSMC parameter is enhanced to disable SMC-D function for the specified port.	Shared Memory Communications - Direct Memory Access
	V2R2	• The SMC parameter is defined to enable SMC-R function for the specified port. This parameter applies only to TCP ports and is required only when AUTOSMC monitoring is in effect. • The NOSMCR parameter has been deprecated but will still be accepted. The NOSMC parameter is the preferred parameter to disable SMC-R function for the specified port.	Shared Memory Communications over RDMA enhancements
	V2R1	The NOSMCR parameter is defined to disable SMC-R function for the specified port.	Shared Memory Communications over Remote Direct Memory Access
PORTRANGE	V2R2	• The SMC parameter is enhanced to enable the SMC-D function. • The NOSMC parameter is enhanced to disable the SMC-D function.	Shared Memory Communications - Direct Memory Access
	V2R2	• The SMC parameter is defined to enable SMC-R function for the specified port. This parameter applies only to TCP ports and is required only when AUTOSMC monitoring is in effect. • The NOSMCR parameter has been deprecated but will still be accepted. The NOSMC parameter is the preferred parameter to disable SMC-R function for the specified port.	Shared Memory Communications over RDMA enhancements
	V2R1	The NOSMCR parameter is defined to disable SMC-R function for the specified port range.	Shared Memory Communications over Remote Direct Memory Access
	V1R13	The *jobname* parameter can now include a 1-7 character prefix followed by a wildcard character (*), enabling all job names that match the prefix to access the ports in the range.	Wildcard support for the PORTRANGE statement

Table 23. Summary of new and changed Communications Server PROFILE.TCPIP configuration statements and parameters (continued)

Statement	Release	Description	Reason for change
SMFCONFIG	V2R1	The SMCRGROUPSTATISTICS and the NOSMCRGROUPSTATISTICS parameters are defined to create SMF 119 subtype 41 interval records for SMC-R link group and link statistics.	Shared Memory Communications over Remote Direct Memory Access
	V2R1	The SMCRLINKEVENT and the NOSMCRLINKEVENT parameters are defined to create SMF 119 subtype 42 and subtype 43 event records for SMC-R link start and end events.	Shared Memory Communications over Remote Direct Memory Access
	V2R1	The IFSTATISTICS and the NOIFSTATISTICS parameters are updated to control the creation of the SMF 119 subtype 44 interval records for IBM 10GbE RoCE Express interface statistics.	Shared Memory Communications over Remote Direct Memory Access
SOMAXCONN	V2R1	Default changed from 10 to 1024.	Enhanced TCP protocol configuration options and default settings

Table 23. Summary of new and changed Communications Server PROFILE.TCPIP configuration statements and parameters (continued)

Statement	Release	Description	Reason for change
TCPCONFIG	V2R2	• AUTODELAYACKS New parameter added to the existing DELAYACKS and NODELAYACKS parameters. Specification of this parameter causes the TCP/IP stack to autonomically determine whether to delay or immediately transmit an acknowledgment when a packet is received with the PUSH bit on in the TCP header. • QUEUEDRTT parameter The default value for the QUEUEDRTT parameter has changed from 20 to 0 milliseconds. • TCPMAXSENDBUFRSIZE parameter Ignored if Outbound right sizing (ORS) is active for a connection.	TCP autonomic tuning enhancements
	V2R1	Added the following new parameters: • CONNECTTIMEOUT • CONNECTINITINTERVAL • FRRTHRESHOLD • KEEPALIVEPROBES • KEEPALIVEPROBEINTERVAL • MAXIMUMRETRANSMITTIME • NAGLE and NONAGLE • QUEUEDRTT • RETRANSMITATTEMPTS • TCPMAXSENDBUFRSIZE • TIMEWAITINTERVAL	Enhanced TCP protocol configuration options and default settings
	V2R1	SELECTIVEACK and NOSELECTIVEACK parameters are added.	TCP support for selective acknowledgements
	V2R1	The EPHEMERALPORTS parameter is added.	User control of Ephmeral Port Ranges
TRANSLATE	V2R2	Support for the HCH and NSAP parameters is removed because the HCH and ATM device types are no longer supported.	Removed support for legacy devices
UDPCONFIG	V2R1	The EPHEMERALPORTS parameter is added.	User control of Ephmeral Port Ranges

Table 23. Summary of new and changed Communications Server PROFILE.TCPIP configuration statements and parameters (continued)

Statement	Release	Description	Reason for change
VIPARANGE	V2R2	The TCP/IP stack can support up to 4096 configured and target DVIPA interfaces instead of 1024. Therefore, more dynamically created DVIPAs can be defined by using a VIPARANGE profile statement.	Increase single stack DVIPA limit to 4096
	V1R13	A new SAF parameter and its associated *resname* value are supported. You can use the SAF parameter to restrict the creation of a dynamic VIPA in the specified VIPARANGE subnet to permitted applications. The maximum number of VIPARANGE statements for one stack is now 1024; prior to V1R13, the maximum number was 256.	Improved security granularity for VIPARANGE DVIPAs

Netstat operator commands (DISPLAY TCPIP,,NETSTAT)

Table 24 lists the new and updated Communications Server IP Netstat operator command DISPLAY TCPIP,,NETSTAT. See Table 25 on page 729 for the other Communications Server IP operator command entries.

See *z/OS Communications Server: IP System Administrator's Commands* for more detailed information about the Communications Server IP operator commands.

All parameters in the following table are for the DISPLAY TCPIP,,NETSTAT operator command.

Table 24. Summary of new and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT)

Parameters	Release	Description	Reason for change
ACCESS,NETWORK	V2R1	The report displays the setting of the new CACHEALL, CACHEPERMIT, and CACHESAME parameters on the NETACCESS statement.	Improve auditing of NetAccess rules

Table 24. Summary of new and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) (continued)

Parameters	Release	Description	Reason for change
ALL	V2R2	• Displays Shared Memory Communications - Direct Memory Access (SMC-D) information for TCP connections. • Accepts the SMCID filter to display the TCP connections that are associated with a specific local SMC-D link identifier.	Shared Memory Communications - Direct Memory Access
	V2R2	Displays new field TcpPrf3. This field is to be used only for diagnostic purposes under the direction of IBM Service personnel.	VIPAROUTE fragmentation avoidance
	V2R2	• Updated the TcpPrf field by adding the description of the dynamic right sizing (DRS) eligible flag bit. • Added new TcpPrf2 field, which describes outbound right sizing (ORS) flag bits. • Added new DelayAck field, which indicates how the TCP/IP stack controls the transmission of acknowledgments for packets received with the PUSH bit on in the TCP header.	TCP autonomic tuning enhancements
	V2R2	New SMC Information section displayed for connections in Listen state.	Shared Memory Communications over RDMA enhancements

Table 24. Summary of new and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) (continued)

Parameters	Release	Description	Reason for change
ALL (continued)	V2R1	Added new StartDate and StartTime fields. These fields provide the date and time for the last of one of the following events: • UDP bind • TCP bind • TCP listen • TCP connection establishment	Socket establishment time for Netstat ALL/-A
	V2R1	Displays the names of the routing policy rule and the policy-based routing table used by IP routing for an IPv6 connection.	IPv6 support for policy-based routing
	V2R1	• Displays Shared Memory Communications through Remote Direct Memory Access (SMC-R) information for TCP connections. • Accepts a new SMCID filter to display only the TCP connections associated with a specific SMC-R link group or SMC-R link identifier.	Shared Memory Communications over Remote Direct Memory Access
	V1R13	The output line that begins with the Last Touched field is now displayed after the output lines for the Bytes, Segments, and Dgram In and Out counters	Release update
	V1R13	Report is enhanced to display the following indicators: • An indicator of whether a TCP connection's send data flow is stalled, SendStalled • An indicator of whether a TCP server is experiencing a potential connection flood attack, ConnectionFlood	Expanded Intrusion Detection Services
ALLCONN	V2R2	Accepts the SMCID filter to display the TCP connections that are associated with a specific local SMC-D link identifier.	Shared Memory Communications - Direct Memory Access
	V2R1	Accepts a new SMCID filter to display only the TCP connections that are associated with a specific SMC-R link group or SMC-R link identifier.	Shared Memory Communications over Remote Direct Memory Access
ARp	V1R13	Displays ARP cache information for an IQDX interface	HiperSockets optimization for intraensemble data networks
CONFIG	V2R2	• Displays new SMCD parameter information in the GLOBALCONFIG section. • Displays new DYNAMICXCF SMCD subparameter information in the IPCONFIG and IPCONFIG6 section.	Shared Memory Communications - Direct Memory Access

Table 24. Summary of new and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) (continued)

Parameters	Release	Description	Reason for change
CONFIG (continued)	V2R2	New field, AdjustDVIPAMSS, under the Global Configuration Information section, displays the setting of the new ADJUSTDVIPAMSS parameter from the GLOBALCONFIG statement.	VIPAROUTE fragmentation avoidance
	V2R2	New SMCGlobal, AutoCache, and AutoSMC fields under the Global Configuration Information section, display the setting of the new SMCGLOBAL parameter and its subparameters from the GLOBALCONFIG statement.	Shared Memory Communications over RDMA enhancements
	V2R2	A new value of Auto can be displayed for the DelayAck field under the TCP Configuration Table section to support the new AUTODELACKS parameter from the TCPCONFIG statement.	TCP autonomic tuning enhancements
	V2R1	Added the following fields to the TCP CONFIGURATION TABLE section: • TimeWaitInterval • RetransmitAttempt • ConnectTimeOut • ConnectInitInterval • Nagle • KeepAliveProbes • KAProbeInterval • QueuedRTT • FRRThreshold • DefltMaxSndBufSize	Enhanced TCP protocol configuration options and default settings
	V2R1	The QDIOAccel indicator reflects "Yes" or "SD only" when IP Security is operational. IP Security introduces additional reasons that QDIOAccel might run in the "SD only" mode.	QDIO acceleration coexistence with IP filtering
	V2R1	The SELECTIVEACK field is added to the TCP CONFIGURATION TABLE section.	TCP support for selective acknowledgements

Table 24. Summary of new and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) (continued)

Parameters	Release	Description	Reason for change
CONFIG (continued)	V2R1	This report displays information about the EPHEMERALPORTS parameter on TCPCONFIG and UDPCONFIG.	User control of Ephmeral Port Ranges
	V2R1	This report displays information about the SOURCEVIPAINTERFACE parameter on IPCONFIG.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	V2R1	• Displays new SMCR parameter information in the GLOBALCONFIG section. • New SmcrGrpStats field in the Type 119 portion of the SMF parameters section indicates whether SMC-R link group statistics records (SMF subtype 41) are collected. • New SmcrLnkEvent field in the Type 119 portion of the SMF parameters section indicates whether the following SMF records are collected: – SMC-R link start (SMF subtype 42) – SMC-R link end (SMF subtype 43)	Shared Memory Communications over Remote Direct Memory Access
	V1R13	New field AutoIQDX added to the Global Configuration section	HiperSockets optimization for intraensemble data networks
	V1R13	• Displays whether checksum offload is globally enabled for IPv4 or IPv6 OSA-Express QDIO interfaces. • Displays whether segmentation offload is globally enabled for IPv4 or IPv6 OSA-Express QDIO interfaces.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	V1R13	The IgRedirect field in the IPv6 Configuration Table section of the report is enhanced. A value of Yes can now indicate that Intrusion Detection Services (IDS) policy is in effect to detect and discard ICMP Redirects.	Expanded Intrusion Detection Services
CONN	V2R2	Accepts the SMCID filter to display the TCP connections that are associated with a specific local SMC-D link identifier.	Shared Memory Communications - Direct Memory Access
	V2R1	Accepts a new SMCID filter to display only the TCP connections that are associated with a specific SMC-R link group or SMC-R link identifier.	Shared Memory Communications over Remote Direct Memory Access

Table 24. Summary of new and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) (continued)

Parameters	Release	Description	Reason for change
DEvlinks	V2R2	• Displays SMC-D information for OSD and HiperSockets interfaces. • Accepts the SMCID filter to display devices that are associated with a specific SMC-D local link identifier. • Accepts the SMC modifier to display detailed SMC-D information about active internal shared memory (ISM) interfaces and their associated SMC-D links. • Accepts the new PNETID modifier to display information about interfaces with a PNETID value, or information about interfaces with a specific PNETID value.	Shared Memory Communications - Direct Memory Access
	V2R2	The following new values can be displayed in the Redundancy field in the SMC Link Group Information section: • Partial (Single local PCHID and port) • Partial (Single local PCHID, unique ports)	Shared Memory Communications over RDMA adapter (RoCE) virtualization

Table 24. Summary of new and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) (continued)

Parameters	Release	Description	Reason for change
DEvlinks (continued)	V2R1	Displays an IP address of 0.0.0.0 for IPAQENET interfaces that are defined with the TEMPIP parameter.	Enable DHCP clients on OSA Interfaces
	V2R1	• Displays Shared Memory Communications over Remote Direct Memory Access information for OSD interfaces. • Accepts a new SMCID filter to display only the devices that are associated with a specific SMC-R link group or SMC-R link identifier. • Accepts a new SMC modifier to display detailed SMC-R information about active RNIC interfaces and their associated SMC-R links and link groups.	Shared Memory Communications over Remote Direct Memory Access
	V2R1	• This report displays information about IPv4 HiperSockets interfaces that are configured with the INTERFACE statement for IPAQIDIO. • This report displays the datapath address and TRLE name for IPAQIDIO6 interfaces, and IPAQIDIO interfaces defined by the INTERFACE statement. • This report displays information about IPv4 static VIPA interfaces that are configured with the INTERFACE statement for VIRTUAL. • The INTFNAME/-K filter accepts a HiperSockets TRLE name that allows for the display of all interfaces for a HiperSockets TRLE.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	V1R13	• Displays whether checksum offload is enabled for an IPAQENET or IPAQENET6 interface. • Displays whether segmentation offload is enabled for an IPAQENET or IPAQENET6 interface.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	V1R13	Displays information about IQDX interfaces.	HiperSockets optimization for intraensemble data networks
HOme	V2R1	Displays a flag value of I/Internal for IPAQENET interfaces that are defined with the TEMPIP parameter.	Enable DHCP clients on OSA Interfaces
	V2R1	The INTFNAME/-K filter accepts a HiperSockets TRLE name that allows for the display of all interfaces for a HiperSockets TRLE.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs

Table 24. Summary of new and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) (continued)

Parameters	Release	Description	Reason for change
IDS	V1R13	Report is enhanced to display the following items: • The ICMPv6 scan rule name in the Scan Detection section • Information about new attack types • The number of TCP servers under a potential connection flood attack, ServersInConnFlood • The number of TCP connections whose send data flow is stalled, TCPStalledConns • The percentage of TCP connections whose send data flow is stalled, TCPStalledConnsPct • An indicator of whether a TCP server is experiencing a potential connection flood attack, ConnFlood in the Intrusion Detection Services TCP Port List section • Both IPv4 and IPv6 addresses in the IP address fields	Expanded Intrusion Detection Services
	V1R13	Report is enhanced to display information about new attack types.	Intrusion Detection Services support for Enterprise Extender
ND	V1R13	Displays neighbor cache information for an IQDX interface.	HiperSockets optimization for intraensemble data networks
PORTLIST	V2R2	Displays a new flag, M, to indicate whether the port or port range is explicitly enabled for SMC-R and SMC-D.	• Shared Memory Communications over RDMA enhancements • Shared Memory Communications - Direct Memory Access
	V2R2	Flag N is enhanced to indicate whether the port or the port range is explicitly disabled for SMC-R and SMC-D.	Shared Memory Communications - Direct Memory Access
	V2R1	Displays a new flag, N, to indicate whether the port or the port range is explicitly disabled for SMC-R.	Shared Memory Communications over Remote Direct Memory Access
ROUTe	V2R1	When the PR=ALL or PR=prname modifier is used to display a policy-based routing table, IPv6 routes are included in the report.	IPv6 support for policy-based routing

Table 24. Summary of new and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) (continued)

Parameters	Release	Description	Reason for change
STATS	V2R2	Displays a new SMCD statistics section. The SMC-D statistics are displayed when no PROTOCOL modifier is specified, or when PROTOCOL=TCP is specified as the modifier value.	Shared Memory Communications - Direct Memory Access
	V2R1	Displays a new SMCR statistics section. The SMC-R statistics are displayed when no PROTOCOL modifier is specified, or when PROTOCOL=TCP is specified as the modifier value.	Shared Memory Communications over Remote Direct Memory Access
	V2R1	This report displays statistics about the usage of ephemeral ports for both TCP and UDP.	User control of Ephmeral Port Ranges
	V1R13	Report is enhanced to display the following information: • The number of TCP connections whose send data flow is stalled, Current Stalled Connections • The number of TCP servers under a potential connection flood attack, Current Servers in Connection Flood	Expanded Intrusion Detection Services
TTLS	V2R2	The report output can have a new value of RFC5280 for CertValidationMode.	AT-TLS certificate processing enhancements
	V2R2	Displays values pertaining to certificate revocation for the new AT-TLS policy agent statements and parameters.	AT-TLS certificate processing enhancements
	V2R2	New fields SessionID and SIDReuseReq provide the session ID and reuse required indicator for FTP connections.	TLS session reuse support for FTP and AT-TLS applications
	V2R1	Reports are updated to show four-character cipher code, TLSv1.2 protocol, and new policy attributes	AT-TLS support for TLS v1.2 and related features
VIPADCFG	V2R2	Report is enhanced to enable the following functions: • Support the MAX= parameter • Display the "n of m records displayed" message.	Release update
	V1R13	The new SAF name field is displayed if the SAF parameter is configured on the VIPARANGE statement.	Improved security granularity for VIPARANGE DVIPAs
VIPADyn	V2R1	When displaying information about DVIPAs with an origin of VIPARANGE IOCTL, an additional field indicates if the DVIPA was created with affinity.	Affinity for application-instance DIVPAs

General updates of IP operator commands

Table 25 lists the new and updated Communications Server IP operator commands, **except** the Netstat operator command DISPLAY TCPIP,,NETSTAT and the Telnet operator commands. See the following tables for those commands:

- Table 24 on page 720, IP Netstat operator commands (DISPLAY TCPIP,,NETSTAT)
- Summary of new and changed Communications Server TN3270E Telnet server operator commands, Telnet operator commands

Table 25. General summary of new and changed Communications Server operator commands

Command	Parameters	Release	Description	Reason for change
DISPLAY TCPIP,,HELP	SMCAT	V2R2	New parameter that provides a help message for the new VARY TCPIP,,SMCAT command syntax.	SMC Applicability Tool (SMCAT)
	TRACE	V2R1	New parameter that provides a help message for the new DISPLAY TCPIP,,TRACE command syntax.	Real-time application-controlled TCP/IP trace NMI

Table 25. General summary of new and changed Communications Server operator commands (continued)

Command	Parameters	Release	Description	Reason for change
DISPLAY TCPIP,,OMPROUTE	IPV6OSPF,IF,NAME=*if_name*	V2R1	The report is enhanced to display the number of IPv6 OSPF packets that are received on the interface that contained errors (# ERR PKTS RCVD), such as bad packet type, bad length, or bad checksum.	Fix OMPROUTE vulnerability to malformed packets
	IPV6OSPF,NBR,ID=*router-id*	V2R1	The report is enhanced to display the number of IPv6 link state advertisements received (# ERR LS RCVD) from the neighbor that were unexpected or contained errors, such as bad advertisement type, bad length, or bad checksum.	Fix OMPROUTE vulnerability to malformed packets
	OSPF,IF,NAME=*if_name*	V2R1	The report is enhanced to display the number of IPv4 OSPF packets that were received on the interface that contained errors (# ERR PKTS RCVD), such as bad packet type, bad length, or bad checksum.	Fix OMPROUTE vulnerability to malformed packets
	OSPF,NBR,IPADDR=*ip_addr*	V2R1	The report is enhanced to display the number of IPv4 link state advertisements received (# ERR LS RCVD) from the neighbor that were unexpected or contained errors, such as bad advertisement type, bad length, or bad checksum.	Fix OMPROUTE vulnerability to malformed packets
	OPTIONS	V2R1	Added new report to display the OMPROUTE GLOBAL_OPTIONS configuration information. Ignore_Undefined_Interfaces is the only one global option.	OMPROUTE adjacency preservation improvements
	RT6TABLE	V2R1	• Added the PRTABLE=ALL parameter to display routes in all OMPROUTE IPv6 policy-based routing tables. • Added the PRTABLE=tablename parameter to display routes in a single OMPROUTE IPv6 policy-based routing table	IPv6 support for policy-based routing

Table 25. General summary of new and changed Communications Server operator commands (continued)

Command	Parameters	Release	Description	Reason for change
DISPLAY TCPIP,,OMPROUTE (continued)	IPV6OSPF,ALL	V1R13	Report includes the new RouterID configuration source definition from an OSPF configuration statement or the assigned interface name. The source is displayed after the RouterID value.	TCP/IP serviceability enhancements
	OSPF,STATISTICS	V1R13	Report includes the new RouterID configuration source definition from an OSPF configuration statement or the assigned interface name. The source is displayed after the RouterID value.	TCP/IP serviceability enhancements
DISPLAY TCPIP,,STOR	N/A	V2R2	Displays the 64-bit storage that is allocated for Shared Memory Communications - Direct Memory Access (SMC-D) processing.	Shared Memory Communications - Direct Memory Access
	N/A	V2R1	Displays the 64-bit storage that is allocated for Shared Memory Communications over Remote Direct Memory Access (SMC-R) processing.	Shared Memory Communications over Remote Direct Memory Access
	N/A	V1R13	Output display is restructured to reflect the 31-bit storage and 64-bit storage usage. See message EZZ8453I for details.	Increased CTRACE and VIT capacity
DISPLAY TCPIP,,TRACE	N/A	V2R1	New command that provides information about applications that are using the Real-time application-controlled TCP/IP trace NMI.	Real-time application-controlled TCP/IP trace NMI
MODIFY CSSMTP	DISPLAY,CONFIG	V2R2	Additional fields in the displayed command output: • DATALINETRUNC • TESTMODE • CONNECTIDLE	CSSMTP migration enablement
	DISPLAY,CONFIG	V2R1	Displays the Header configuration statement	CSSMTP mail message date header handling option
	FLUSHRetry,AGE=*day*	V1R13	Flush extended retry mail over AGE= days old.	CSSMTP extended retry
	DISPLAY,CONFIG	V1R13	Displays the new JESSyntaxErrLimit statement value.	CSSMTP enhancements
MODIFY DMD	DISPLAY	V2R1	The display output includes the setting of the new DefaultLogLimit parameter.	Limit defensive filter logging
	REFRESH	V2R1	The value of the new DefaultLogLimit parameter can be changed by updating the DMD configuration file and issuing MODIFY DMD,REFRESH.	Limit defensive filter logging

Table 25. General summary of new and changed Communications Server operator commands (continued)

Command	Parameters	Release	Description	Reason for change
MODIFY OMPROUTE	IPV6OSPF,ALL	V1R13	Report includes the new RouterID configuration source definition from an OSPF configuration statement or the assigned interface name. The source is displayed after the RouterID value.	TCP/IP serviceability enhancements
	OSPF,STATISTICS	V1R13	Report includes the new RouterID configuration source definition from an OSPF configuration statement or the assigned interface name. The source is displayed after the RouterID value.	TCP/IP serviceability enhancements
MODIFY omproute_procname	RT6TABLE	V2R1	• Added the PRTABLE=ALL parameter to display routes in all OMPROUTE IPv6 policy-based routing tables. • Added the PRTABLE=tablename parameter to display routes in a single OMPROUTE IPv6 policy-based routing table	IPv6 support for policy-based routing
MODIFY RESOLVER	DISPLAY	V2R2	When system caching is active, an additional instance of message EZZ9304I is included to display the current system-wide cache reordering setting. One of the following values is displayed: • CACHEREORDER • NOCACHEREORDER	Reordering of cached Resolver results
	DISPLAY	V1R13	When the autonomic quiesce of unresponsive name servers function is active, message EZD2035I is displayed for each name server in the global TCPIP.DATA file.	System resolver autonomic quiescing of unresponsive name servers
	REFRESH[,SETUP=]	V2R2	Changed to display the new system-wide cache reordering setting. One of the following values is displayed: • CACHEREORDER • NOCACHEREORDER	Reordering of cached Resolver results
	REFRESH[,SETUP=]	V1R13	When the autonomic quiesce of unresponsive name servers function is active after completion of the MODIFY command processing, message EZD2035I is displayed for each name server in the global TCPIP.DATA file.	System resolver autonomic quiescing of unresponsive name servers

Table 25. General summary of new and changed Communications Server operator commands (continued)

Command	Parameters	Release	Description	Reason for change
VARY TCPIP,,SMCAT	N/A	V2R2	New command used to turn the SMC Applicability Tool on or off. The SMC Applicability Tool monitors TCP connections to determine their eligibility to use SMC communications.	SMC Applicability Tool (SMCAT)
VARY TCPIP,,SYNTAXCHECK	N/A	V2R1	New command that can be used to check the syntax of TCP/IP profile configuration statements without affecting the system operation or network configuration.	Check TCP/IP profile syntax without applying configuration changes

NETSTAT TSO commands

Table 26 lists the new and updated Communications Server NETSTAT TSO command.

See *z/OS Communications Server: IP System Administrator's Commands* for more detailed information about the Communications Server TSO commands.

Table 26. Summary of new and changed Communications Server NETSTAT TSO commands

Parameter	Release	Description	Reason for change
ALL	V2R2	• Displays Shared Memory Communications - Direct Memory Access (SMC-D) information for TCP connections. • Accepts the SMCID filter to display the TCP connections that are associated with a specific local SMC-D link identifier.	Shared Memory Communications - Direct Memory Access
	V2R2	Displays new field TcpPrf3. This field is to be used only for diagnostic purposes under the direction of IBM Service personnel.	VIPAROUTE fragmentation avoidance
	V2R2	New SMC Information section displayed for connections in Listen state.	Shared Memory Communications over RDMA enhancements
	V2R2	• Updated the TcpPrf field by adding the description of the dynamic right sizing (DRS) eligible flag bit. • Added new TcpPrf2 field, which describes outbound right sizing (ORS) flag bits. • Added new DelayAck field, which indicates how the TCP/IP stack controls the transmission of acknowledgments for packets received with the PUSH bit on in the TCP header.	TCP autonomic tuning enhancements

Table 26. Summary of new and changed Communications Server NETSTAT TSO commands (continued)

Parameter	Release	Description	Reason for change
ALL (continued)	V2R1	Added new StartDate and StartTime fields. These fields provide the date and time for the last of one of the following events: • UDP bind time • TCP bind time • TCP listen time • TCP connection establishment time	Socket establishment time for Netstat ALL/-A
	V2R1	Displays the names of the routing policy rule and the policy-based routing table used by IP routing for an IPv6 connection	IPv6 support for policy-based routing
	V2R1	• Displays Shared Memory Communications over Remote Direct Memory Access (SMC-R) information for TCP connections. • Accepts a new SMCLID filter to display only the TCP connections associated with a specific SMC-R link group or SMC-R link identifier.	Shared Memory Communications over Remote Direct Memory Access
	V1R13	The output line that begins with the Last Touched field is now displayed after the output lines for the Bytes, Segments, and Dgram In and Out counters	Release update
	V1R13	Report is enhanced to display the following indicators: • The number of TCP connections whose send data flow is stalled, Current Stalled Connections • The number of TCP servers under a potential connection flood attack, Current Servers in Connection Flood	Expanded Intrusion Detection Services
ALLCONN	V2R2	Accepts the SMCID filter to display the TCP connections that are associated with a specific local SMC-D link identifier.	Shared Memory Communications - Direct Memory Access
	V2R1	Accepts a new SMCID filter to display only the TCP connections that are associated with a specific SMC-R link group or SMC-R link identifier.	Shared Memory Communications over Remote Direct Memory Access
ARp	V1R13	Displays ARP cache information for an IQDX interface.	HiperSockets optimization for intraensemble data networks

Table 26. Summary of new and changed Communications Server NETSTAT TSO commands (continued)

Parameter	Release	Description	Reason for change
CONFIG	V2R2	• Displays new SMCD parameter information in the GLOBALCONFIG section. • Displays new DYNAMICXCF SMCD subparameter information in the IPCONFIG and IPCONFIG6 section.	Shared Memory Communications - Direct Memory Access
	V2R2	New field, AdjustDVIPAMSS, under the Global Configuration Information section, displays the setting of the new ADJUSTDVIPAMSS parameter from the GLOBALCONFIG statement.	VIPAROUTE fragmentation avoidance
	V2R2	New SMCGlobal, AutoCache, and AutoSMC fields under the Global Configuration Information section, display the setting of the new SMCGLOBAL parameter and its subparameters from the GLOBALCONFIG statement.	Shared Memory Communications over RDMA enhancements
	V2R2	A new value of Auto can be displayed for the DelayAck field under the TCP Configuration Table section to support the new AUTODELACKS parameter from the TCPCONFIG statement.	TCP autonomic tuning enhancements

Table 26. Summary of new and changed Communications Server NETSTAT TSO commands (continued)

Parameter	Release	Description	Reason for change
CONFIG (continued)	V2R1	Added the following fields to the TCP CONFIGURATION TABLE section: • TimeWaitInterval • RetransmitAttempt • ConnectTimeOut • ConnectInitInterval • Nagle • KeepAliveProbes • KAProbeInterval • QueuedRTT • FRRThreshold • DefltMaxSndBufSize	Enhanced TCP protocol configuration options and default settings
	V2R1	• Displays new SMCR parameter information in the GLOBALCONFIG section. • New SmcrGrpStats field in the Type 119 portion of the SMF parameters section indicates whether SMC-R link group statistics records (SMF subtype 41) are collected. • New SmcrLnkEvent field in the Type 119 portion of the SMF parameters section indicates whether the following SMF records are collected: – SMC-R link start (SMF subtype 42) – SMC-R link end (SMF subtype 43)	Shared Memory Communications over Remote Direct Memory Access
	V2R1	The QDIOAccel indicator reflects "Yes" or "SD only" when IP Security is operational. IP Security introduces additional reasons that QDIOAccel might run in the "SD only" mode.	QDIO acceleration coexistence with IP filtering
	V2R1	The SELECTIVEACK field is added to the TCP Configuration Table section.	TCP support for selective acknowledgements
	V2R1	This report displays information about the EPHEMERALPORTS parameter on TCPCONFIG and UDPCONFIG.	User control of Ephmeral Port Ranges
	V2R1	This report displays information about the SOURCEVIPAINTERFACE parameter on IPCONFIG.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	V1R13	New field AutoIQDX added to the Global Configuration section.	HiperSockets optimization for intraensemble data networks
	V1R13	• Displays whether checksum offload is globally enabled for IPv4 or IPv6 OSA-Express QDIO interfaces. • Displays whether segmentation offload is globally enabled for IPv4 or IPv6 OSA-Express QDIO interfaces.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	V1R13	The IgRedirect field in the IPv6 Configuration Table section of the report is enhanced. A value of Yes can now indicate that Intrusion Detection Services (IDS) policy is in effect to detect and discard ICMP Redirects.	Expanded Intrusion Detection Services

Table 26. Summary of new and changed Communications Server NETSTAT TSO commands (continued)

Parameter	Release	Description	Reason for change
CONN	V2R2	Accepts the SMCID filter to display the TCP connections that are associated with a specific local SMC-D link identifier.	Shared Memory Communications - Direct Memory Access
	V2R1	Accepts a new SMCID filter to display only the TCP connections that are associated with a specific SMC-R link group or SMC-R link identifier.	Shared Memory Communications over Remote Direct Memory Access
DEvlinks	V2R2	• Displays SMC-D information for OSD and HiperSockets interfaces. • Accepts the SMCID filter to display devices that are associated with a specific SMC-D local link identifier. • Accepts the SMC modifier to display detailed SMC-D information about active internal shared memory (ISM) interfaces and their associated SMC-D links. • Accepts the new PNETID modifier to display information about interfaces with a PNETID value, or information about interfaces with a specific PNETID value.	Shared Memory Communications - Direct Memory Access
	V2R2	The following new values can be displayed in the Redundancy field in the SMC Link Group Information section: • Partial (Single local PCHID and port) • Partial (Single local PCHID, unique ports)	Shared Memory Communications over RDMA adapter (RoCE) virtualization
	V2R1	Displays an IP address of 0.0.0.0 for IPAQENET interfaces that are defined with the TEMPIP parameter.	Enable DHCP clients on OSA Interfaces
	V2R1	• This report displays information about IPv4 HiperSockets interfaces that are configured with the INTERFACE statement for IPAQIDIO. • This report displays information about IPv4 static VIPA interfaces that are configured with the INTERFACE statement for VIRTUAL. • The INTFNAME/-K filter accepts a HiperSockets TRLE name that allows for the display of all interfaces for a HiperSockets TRLE.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	V2R1	• Displays Shared Memory Communications over Remote Direct Memory Access (SMC-R) information for OSD interfaces. • Accepts a new SMCID filter to display only the devices that are associated with a specific SMC-R link group or SMC-R link identifier. • Accepts a new SMC modifier to display detailed SMC-R information about active RNIC interfaces and their associated SMC-R links and link groups.	Shared Memory Communications over Remote Direct Memory Access
DEvlinks (continued)	V1R13	Displays information about IQDX interfaces.	HiperSockets optimization for intraensemble data networks
	V1R13	• Displays whether checksum offload is enabled for an IPAQENET or IPAQENET6 interface. • Displays whether segmentation offload is enabled for an IPAQENET or IPAQENET6 interface.	OSA-Express4S QDIO IPv6 checksum and segmentation offload

Table 26. Summary of new and changed Communications Server NETSTAT TSO commands (continued)

Parameter	Release	Description	Reason for change
HOme	V2R1	Displays a flag value of I/Internal for IPAQENET interfaces that are defined with the TEMPIP parameter.	Enable DHCP clients on OSA Interfaces
	V2R1	The INTFNAME/-K filter accepts a HiperSockets TRLE name that allows for the display of all interfaces for a HiperSockets TRLE.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
IDS	V1R13	Report is enhanced to display the following information: • The ICMPv6 scan rule name in the Scan Detection section • Information about new attack types • The number of TCP servers under a potential connection flood attack, ServersInConnFlood • The number of TCP connections whose send data flow is stalled, TCPStalledConns • The percentage of TCP connections whose send data flow is stalled, TCPStalledConnsPct • An indicator of whether a TCP server is experiencing a potential connection flood attack, ConnFlood in the Intrusion Detection Services TCP Port List section • Both IPv4 and IPv6 addresses in the IP address fields	Expanded Intrusion Detection Services
	V1R13	Report is enhanced to display information about new attack types.	Intrusion Detection Services support for Enterprise Extender
ND	V1R13	Displays Neighbor cache information for an IQDX interface.	HiperSockets optimization for intraensemble data networks
PORTLIST	V2R2	Displays a new flag, M, to indicate whether the port or port range is explicitly enabled for SMC-R and SMC-D.	• Shared Memory Communications over RDMA enhancements • Shared Memory Communications - Direct Memory Access
	V2R2	Flag N is enhanced to indicate whether the port or the port range is explicitly disabled for SMC-R and SMC-D.	Shared Memory Communications - Direct Memory Access
	V2R1	Displays a new flag, N, to indicate whether the port or the port range is explicitly disabled for SMC-R.	Shared Memory Communications over Remote Direct Memory Access
ROUTe	V2R1	When the PR=ALL or PR=prname modifier is used to display a policy-based routing table, IPv6 routes are included in the report.	IPv6 support for policy-based routing

Table 26. Summary of new and changed Communications Server NETSTAT TSO commands (continued)

Parameter	Release	Description	Reason for change
STATS	V2R2	Displays a new SMCD statistics section. The SMC-D statistics are displayed when no PROTOCOL modifier is specified, or when PROTOCOL=TCP is specified as the modifier value.	Shared Memory Communications - Direct Memory Access
	V2R1	Displays a new SMCR statistics section. The SMC-R statistics are displayed when no PROTOCOL modifier is specified, or when PROTOCOL=TCP is specified as the modifier value.	Shared Memory Communications over Remote Direct Memory Access
	V2R1	This report displays statistics about the usage of ephemeral ports for both TCP and UDP.	User control of Ephmeral Port Ranges
	V1R13	Report is enhanced to display the following information: • The number of TCP connections whose send data flow is stalled, Current Stalled Connections • The number of TCP servers under a potential connection flood attack, Current Servers in Connection Flood	Expanded Intrusion Detection Services
TTLS	V2R2	The report output can have a new value of RFC5280 for CertValidationMode.	AT-TLS certificate processing enhancements
	V2R2	Displays values pertaining to certificate revocation for the new AT-TLS policy agent statements and parameters.	AT-TLS certificate processing enhancements
	V2R2	New fields SessionID and SIDReuseReq provide the session ID and reuse required indicator for FTP connections.	TLS session reuse support for FTP and AT-TLS applications
	V2R1	Reports are updated to show four-character cipher code, TLSv1.2 protocol, and new policy attributes.	AT-TLS support for TLS v1.2 and related features
VIPADCFG	V1R13	The new SAF name field is displayed if the SAF parameter is configured on the VIPARANGE statement.	Improved security granularity for VIPARANGE DVIPAs
VIPADyn	V2R1	When displaying information about DVIPAs with an origin of VIPARANGE IOCTL, an additional field indicates if the DVIPA was created with affinity.	Affinity for application-instance DIVPAs

Netstat UNIX commands

Table 27 on page 740 lists the new and updated Communications Server z/OS UNIX netstat command. See Summary of new and changed Communications Server z/OS UNIX commands for the other (the non-netstat) z/OS UNIX command entries.

See *z/OS Communications Server: IP System Administrator's Commands* for more detailed information about the z/OS UNIX commands.

All parameters in the following table are for the z/OS UNIX netstat command.

Table 27. Summary of new and changed Communications Server z/OS UNIX netstat commands

Parameter	Release	Description	Reason for change
-A	V2R2	• Displays Shared Memory Communications - Direct Memory Access (SMC-D) information for TCP connections. • Accepts the SMCID filter to display the TCP connections that are associated with a specific local SMC-D link identifier.	Shared Memory Communications - Direct Memory Access
	V2R2	Displays new field TcpPrf3. This field is to be used only for diagnostic purposes under the direction of IBM Service personnel.	VIPAROUTE fragmentation avoidance
	V2R2	New SMC Information section displayed for connections in Listen state.	Shared Memory Communications over RDMA enhancements
	V2R2	• Updated TcpPrf field by adding the description of the dynamic right sizing (DRS) eligible flag bit. • Added new TcpPrf2 field, which describes outbound right sizing (ORS) flag bits. • Added new DelayAck field, which indicates how the TCP/IP stack controls the transmission of acknowledgments for packets received with the PUSH bit on in the TCP header.	TCP autonomic tuning enhancements
-A (continued)	V2R1	Added new StartDate and StartTime fields. These fields provide the date and time for the last of one of the following events: • UDP bind time • TCP bind time • TCP listen time • TCP connection establishment time	Socket establishment time for Netstat ALL/-A
	V2R1	Displays the names of the routing policy rule and the policy-based routing table used by IP routing for an IPv6 connection	IPv6 support for policy-based routing
	V2R1	• Displays Shared Memory Communications over Remote Direct Memory Access (SMC-R) information for TCP connections. • Accepts a new -U filter to display only the TCP connections associated with a specific SMC-R link group or SMC-R link identifier.	Shared Memory Communications over Remote Direct Memory Access
	V1R13	The output line that begins with the Last Touched field is now displayed after the output lines for the Bytes, Segments, and Dgram In and Out counters	Release update
	V1R13	Report is enhanced to display the following indicators: • An indicator of whether a TCP connection's send data flow is stalled, SendStalled • An indicator of whether a TCP server is experiencing a potential connection flood attack, ConnectionFlood	Expanded Intrusion Detection Services

Table 27. Summary of new and changed Communications Server z/OS UNIX netstat commands (continued)

Parameter	Release	Description	Reason for change
-a	V2R2	Accepts the SMCID filter to display the TCP connections that are associated with a specific local SMC-D link identifier.	Shared Memory Communications - Direct Memory Access
	V2R1	Accepts a new -U filter to display only the TCP connections that are associated with a specific SMC-R link group or SMC-R link identifier.	Shared Memory Communications over Remote Direct Memory Access
-c	V2R2	Accepts the SMCID filter to display the TCP connections that are associated with a specific local SMC-D link identifier.	Shared Memory Communications - Direct Memory Access
	V2R1	Accepts a new -U filter to display only the TCP connections that are associated with a specific SMC-R link group or SMC-R link identifier.	Shared Memory Communications over Remote Direct Memory Access

Table 27. Summary of new and changed Communications Server z/OS UNIX netstat commands (continued)

Parameter	Release	Description	Reason for change
-d	V2R2	• Displays SMC-D information for OSD and HiperSockets interfaces. • Accepts the SMCID filter to display devices that are associated with a specific SMC-D local link identifier. • Accepts the SMC modifier to display detailed SMC-D information about active internal shared memory (ISM) interfaces and their associated SMC-D links. • Accepts the new PNETID modifier to display information about interfaces with a PNETID value, or information about interfaces with a specific PNETID value.	Shared Memory Communications - Direct Memory Access
	V2R2	The following new values can be displayed in the Redundancy field in the SMC Link Group Information section: • Partial (Single local PCHID and port) • Partial (Single local PCHID, unique ports)	Shared Memory Communications over RDMA adapter (RoCE) virtualization
	V2R1	Displays an IP address of 0.0.0.0 for IPAQENET interfaces that are defined with the TEMPIP parameter.	Enable DHCP clients on OSA Interfaces
	V2R1	• Displays Shared Memory Communications over Remote Direct Memory Access information for OSD interfaces. • Accepts a new -U filter to display only the devices associated with a specific SMC-R link group or SMC-R link identifier. • Accepts a new SMC modifier to display detailed SMC-R information about active RNIC interfaces and their associated SMC-R links and link groups.	Shared Memory Communications over Remote Direct Memory Access
	V2R1	• This report displays information about IPv4 HiperSockets interfaces that are configured with the INTERFACE statement for IPAQIDIO. • This report displays the datapath address and TRLE name for IPAQIDIO6 interfaces, and IPAQIDIO interfaces defined by the INTERFACE statement. • This report displays information about IPv4 static VIPA interfaces that are configured with the INTERFACE statement for VIRTUAL. • The INTFNAME/-K filter accepts a HiperSockets TRLE name that allows for the display of all interfaces for a HiperSockets TRLE.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	V1R13	• Displays whether checksum offload is globally enabled for IPv4 or IPv6 OSA-Express QDIO interfaces. • Displays whether segmentation offload is globally enabled for IPv4 or IPv6 OSA-Express QDIO interfaces.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	V1R13	Displays information about IQDX interfaces	HiperSockets optimization for intraensemble data networks
-F	V1R13	The new SAF name field is displayed if the SAF parameter is configured on the VIPARANGE statement.	Improved security granularity for VIPARANGE DVIPAs

Table 27. Summary of new and changed Communications Server z/OS UNIX netstat commands (continued)

Parameter	Release	Description	Reason for change
-f	V2R2	• Displays new SMCD parameter information in the GLOBALCONFIG section. • Displays new DYNAMICXCF SMCD subparameter information in the IPCONFIG and IPCONFIG6 section.	Shared Memory Communications - Direct Memory Access
	V2R2	New field, AdjustDVIPAMSS, under the Global Configuration Information section, displays the setting of the new ADJUSTDVIPAMSS parameter from the GLOBALCONFIG statement.	VIPAROUTE fragmentation avoidance
	V2R2	New SMCGlobal, AutoCache, and AutoSMC fields under the Global Configuration Information section, display the setting of the new SMCGLOBAL parameter and its subparameters from the GLOBALCONFIG statement.	Shared Memory Communications over RDMA enhancements
	V2R2	A new value of Auto can be displayed for the DelayAck field under the TCP Configuration Table section to support the new AUTODELACKS parameter from the TCPCONFIG statement.	TCP autonomic tuning enhancements
	V2R1	Added the following fields to the TCP CONFIGURATION TABLE section: • TimeWaitInterval • RetransmitAttempt • ConnectTimeOut • ConnectInitInterval • Nagle • KeepAliveProbes • KAProbeInterval • QueuedRTT • FRRThreshold • DefltMaxSndBufSize	Enhanced TCP protocol configuration options and default settings

Table 27. Summary of new and changed Communications Server z/OS UNIX netstat commands (continued)

Parameter	Release	Description	Reason for change
-f (continued)-h	V2R1	• Displays new SMCR parameter information in the GLOBALCONFIG section. • New SmcrGrpStats field in the Type 119 portion of the SMF parameters section indicates whether SMC-R link group statistics records (SMF subtype 41) are collected. • New SmcrLnkEvent field in the Type 119 portion of the SMF parameters section indicates whether the following SMF records are collected: – SMC-R link start (SMF subtype 42) – SMC-R link end (SMF subtype 43)	Shared Memory Communications over Remote Direct Memory Access
	V2R1	The QDIOAccel indicator reflects "Yes" or "SD only" when IP Security is operational. IP Security introduces additional reasons that QDIOAccel might run in the "SD only" mode.	QDIO acceleration coexistence with IP filtering
	V2R1	This report displays information about the EPHEMERALPORTS parameter on TCPCONFIG and UDPCONFIG.	User control of Ephmeral Port Ranges
	V2R1	The SELECTIVEACK field is added to the TCP Configuration Table section.	TCP support for selective acknowledgements
	V2R1	This report displays information about the SOURCEVIPAINTERFACE parameter on IPCONFIG.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	V1R13	• Displays whether checksum offload is globally enabled for IPv4 or IPv6 OSA-Express QDIO interfaces. • Displays whether segmentation offload is globally enabled for IPv4 or IPv6 OSA-Express QDIO interfaces.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	V1R13	New field AutoIQDX added to the Global Configuration section.	HiperSockets optimization for intraensemble data networks
	V1R13	The IgRedirect field in the IPv6 Configuration Table section of the report is enhanced. A value of Yes can now indicate that Intrusion Detection Services (IDS) policy is in effect to detect and discard ICMP Redirects.	Expanded Intrusion Detection Services
	V2R1	Displays a flag value of I/Internal for IPAQENET interfaces that are defined with the TEMPIP parameter.	Enable DHCP clients on OSA Interfaces
	V2R1	The INTFNAME/-K filter accepts a HiperSockets TRLE name that allows for the display of all interfaces for a HiperSockets T-RLE.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs

Table 27. Summary of new and changed Communications Server z/OS UNIX netstat commands (continued)

Parameter	Release	Description	Reason for change
-k	V1R13	Report is enhanced to display the following information: • The ICMPv6 scan rule name in the Scan Detection section • Information about new attack types • The number of TCP servers under a potential connection flood attack, ServersInConnFlood • The number of TCP connections whose send data flow is stalled, TCPStalledConns • The percentage of TCP connections whose send data flow is stalled, TCPStalledConnsPct • An indicator of whether a TCP server is experiencing a potential connection flood attack, ConnFlood in the Intrusion Detection Services TCP Port List section • Both IPv4 and IPv6 addresses in the IP address fields	Expanded Intrusion Detection Services
	V1R13	Report is enhanced to display information about new attack types.	Intrusion Detection Services support for Enterprise Extender
-n	V1R13	Displays neighbor cache information for an IQDX interface.	HiperSockets optimization for intraensemble data networks
-o	V2R2	Displays a new flag, M, to indicate whether the port or port range is explicitly enabled for SMC-R and SMC-D.	• Shared Memory Communications over RDMA enhancements • Shared Memory Communications - Direct Memory Access
	V2R2	Flag N is enhanced to indicate whether the port or the port range is explicitly disabled for SMC-R and SMC-D.	Shared Memory Communications - Direct Memory Access
	V2R1	Displays a new flag, N, to indicate whether the port or the port range is explicitly disabled for SMC-R.	Shared Memory Communications over Remote Direct Memory Access
-r	V2R1	When the PR=ALL or PR=prname modifier is used to display a policy-based routing table, IPv6 routes are included in the report.	IPv6 support for policy-based routing
	V1R13	Displays ARP cache information for an IQDX interface.	HiperSockets optimization for intraensemble data networks

Table 27. Summary of new and changed Communications Server z/OS UNIX netstat commands (continued)

Parameter	Release	Description	Reason for change
-S	V2R2	Displays a new SMCD statistics section. The SMC-D statistics are displayed when no PROTOCOL modifier is specified, or when PROTOCOL=TCP is specified as the modifier value.	Shared Memory Communications - Direct Memory Access
	V2R1	Displays a new SMCR statistics section. The SMC-R statistics are displayed when no PROTOCOL modifier is specified, or when PROTOCOL=TCP is specified as the modifier value.	Shared Memory Communications over Remote Direct Memory Access
	V2R1	This report displays statistics about the usage of ephemeral ports for both TCP and UDP.	User control of Ephmeral Port Ranges
	V1R13	Report is enhanced to display the following information: • The number of TCP connections whose send data flow is stalled, Current Stalled Connections • The number of TCP servers under a potential connection flood attack, Current Servers in Connection Flood	Expanded Intrusion Detection Services
-v	V2R1	When displaying information about DVIPAs with an origin of VIPARANGE IOCTL, an additional field indicates if the DVIPA was created with affinity.	Affinity for application-instance DIVPAs
-x	V2R2	The report output can have a new value of RFC5280 for CertValidationMode.	AT-TLS certificate processing enhancements
	V2R2	Displays values pertaining to certificate revocation for the new AT-TLS policy agent statements and parameters.	AT-TLS certificate processing enhancements
	V2R2	New fields SessionID and SIDReuseReq provide the session ID and reuse required indicator for FTP connections.	TLS session reuse support for FTP and AT-TLS applications
	V2R1	Reports are updated to show four-character cipher code, TLSv1.2 protocol, and new policy attributes	AT-TLS support for TLS v1.2 and related features

TCP/IP callable NMI (EZBNMIFR)

Table 28 on page 747 lists the updates to the Communications Server TCP/IP callable NMI.

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR)

Request	Parameter/output	Rel.	Description	Reason for change
GetConnectionDetail	• NWMConnFlag01 – NWMConnSMCDCfg • NWMConnSMCDStatus • NWMConnSMCDReason • NWMConnSMCFlags – NWMConnSMCDRsnRmt • NWMConnSMCFlags – NWMConnSMCDCached • NWMConnLclSMCLinkId • NWMConnRmtSMCLinkId	V2R2	• New flag bit NWMConnSMCDCfg is set in the NWMConnFlag01 field to indicate whether the SMCD parameter is configured on the GLOBALCONFIG statement. • New NWMConnSMCDStatus field that indicates whether this connection is traversing an SMC-D link. • New NWMConnSMCDReason field that indicates why a connection is not using an SMC-D link. • New flag bit NWMConnSMCDRsnRmt is set in the NWMConnSMCFlags field to indicate whether the NWMConnSMCDReason is set by the remote peer. • New flag bit NWMConnSMCDCached is set in the NWMConnSMCFlags field to indicate whether this connection is cached to not use SMC-D. • Existing NWMConnLclSMCLinkId field that indicates the local stack link ID for the SMC-R or SMC-D link that this connection traverses. • Existing NWMConnRmtSMCLinkId field that indicates the remote stack link ID for the SMC-R or SMC-D link that this connection traverses.	Shared Memory Communications - Direct Memory Access

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetConnectionDetail (continued)	NWMConnFlag01	V2R2	Added the following new flag bits to field NWMConnFlag01: • NWMConnDRSEligible • NWMConnDRSActive	TCP autonomic tuning enhancements
	NWMConnFlag02	V2R2	Added a new flag byte field, NWMConnFlag02, with the following flag bits: • NWMConnORSEligible • NWMConnORSActive • NWMConnORSSndBufExp • NWMConnAutoDelayAck • NWMConnDelayAck	TCP autonomic tuning enhancements
	NWMConnLclSMCBufSz	V2R2	Existing NWMConnLclSMCBufSz field that indicates the size of the RMB or DMB element that the local host uses to receive data on this connection from the remote host.	• Shared Memory Communications over RDMA enhancements • Shared Memory Communications - Direct Memory Access
	NWMConnRmtSMCBufSz	V2R2	Existing NWMConnRmtSMCBufSz field that indicates the size of the RMB or DMB element that the remote host uses to receive data on this connection from the local host.	• Shared Memory Communications over RDMA enhancements • Shared Memory Communications - Direct Memory Access
	NWMConnSMCFlags	V2R2	Added a new flag bit NWMConnSMCCached.	Shared Memory Communications over RDMA enhancements
	NWMConnSMCReason	V2R2	Added a new constant NWMSMCRSNAUTOSMCR.	Shared Memory Communications over RDMA enhancements
	NWMConnLclSMCLinkId	V2R1	New NWMConnLclSMCLinkId field that indicates the local stack link ID for the SMC-R link that this connection traverses.	Shared Memory Communications over Remote Direct Memory Access
	NWMConnRmtSMCLinkId	V2R1	New NWMConnRmtSMCLinkId field that indicates the remote stack link ID for the SMC-R link that this connection traverses.	Shared Memory Communications over Remote Direct Memory Access
	NWMConnSMCRCfg	V2R1	New flag bit NWMConnSMCRCfg is set in the NWMConnFlag01 field to indicate whether the SMCR parameter is configured on the GLOBALCONFIG statement.	Shared Memory Communications over Remote Direct Memory Access
	NWMConnSMCReason	V2R1	New NWMConnSMCReason field that indicates why a connection is not using an SMC-R link.	Shared Memory Communications over Remote Direct Memory Access
	NWMConnSMCStatus	V2R1	New NWMConnSMCStatus field that indicates whether this connection is traversing an SMC-R link.	Shared Memory Communications over Remote Direct Memory Access
	NWMConnTTLSSSLProt	V2R1	New NWMTTLSPROTTLSV1_2 value (X'0303').	AT-TLS support for TLS v1.2 and related features
	NWMConnTTLSSSLNegCiph	V2R1	New NWMTTLSNEGCIPH4X value (X'4X') is added to indicate four-character cipher.	AT-TLS support for TLS v1.2 and related features
	NWMConnTTLSSSLNegCiph4	V2R1	New field containing four-character negotiated cipher code.	AT-TLS support for TLS v1.2 and related features
	NWMConnStall	V1R13	New bit defined that indicates whether the connection's send data flow is stalled.	Expanded Intrusion Detection Services

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetDVIPAList	NWMDvListFlags	V2R1	A new flag, NWMDVLISTFLAGS_DVRAFFINITY (0x04), is added. The flag means that an application instance DVIPA was created with affinity. Applications are permitted to dynamically create DVIPAs that are within the range defined by a VIPARANGE statement.	Affinity for application-instance DIVPAs
GetFTPDaemonConfig	SMF119FT_FDCFSecSessReuse	V2R2	New SMF119FT_FDCFSecSessReuse field contains the value of the statement SECURE_SESSION_REUSE in the server FTP.DATA.	TLS session reuse support for FTP and AT-TLS applications
	SMF119FT_FDCFApplname	V2R1	New SMF119FT_FDCFApplname field contains 8-character FTP server application name from the APPLNAME statement.	Release update
	SMF119FT_FDCFSslv3	V2R1	New field to enable or disable SSLV3	APAR PI28679
	N/A	V2R1	New poll-type request to provide FTP daemon configuration information.	NMI and SMF enhancements for TCP/IP applications

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetGlobalStats	NWMTCPSTSMCDCfg Existing TCP stats changed: NWMTCPSTCurrEstab NWMTCPSTActiveOpened NWMTCPSTPassiveOpened NWMTCPSTConnClosed NWMTCPSTInSegs NWMTCPSTOutSegs NWMTCPSTOutRsts NWMTCPSTEstabResets NWMTCPSTAcceptCount NWMTCPSTKeepAliveProbes NWMTCPSTKeepAliveDrop NWMTCPSTFinwait2Drops New SMC-D stats: NWMTCPSTSMCDCurrEstabLnks NWMTCPSTSMCDActLnkOpened NWMTCPSTSMCDPasLnkOpened NWMTCPSTSMCDLnksClosed NWMTCPSTSMCDCurrEstab NWMTCPSTSMCDActiveOpened NWMTCPSTSMCDPassiveOpened NWMTCPSTSMCDConnClosed NWMTCPSTSMCRInSegs NWMTCPSTSMCROutSegs NWMTCPSTSMCRInRsts NWMTCPSTSMCROutRsts	V2R2	• New flag bit NWMTCPSTSMCDCfg is set in the NWMTCPSTFlags field to indicate whether SMC-D processing is or has been in effect. • When the NWMTCPSTSMCDCfg flag is set, the listed TCP counters reflect all TCP connections, including connections over SMC-D links. • The listed SMC-D statistics are added.	Shared Memory Communications - Direct Memory Access
	NWMTCPSTCfgEphemDef	V2R1	Contains the number of configured ephemeral ports to be assigned for TCP applications.	User control of Ephmeral Port Ranges
	NWMTCPSTEphemInUse	V2R1	Contains the current number of configured ephemeral ports in use by TCP applications.	User control of Ephmeral Port Ranges
	NWMTCPSTEphemHiWater	V2R1	Contains the highest number of configured ephemeral ports in use by TCP applications at any time.	User control of Ephmeral Port Ranges
	NWMTCPSTEphemExhaust	V2R1	Contains the number of bind() requests that failed because no TCP ephemeral port was available.	User control of Ephmeral Port Ranges
	NWMUDPSTCfgEphemDef	V2R1	Contains the number of configured ephemeral ports to be assigned for UDP applications.	User control of Ephmeral Port Ranges
	NWMUDPSTEphemInUse	V2R1	Contains the current number of configured ephemeral ports in use by UDP applications.	User control of Ephmeral Port Ranges
	NWMUDPSTEphemHiWater	V2R1	Contains the highest number of configured ephemeral ports in use by UDP applications at any time.	User control of Ephmeral Port Ranges
	NWMUDPSTEphemExhaust	V2R1	Contains the number of bind() requests that failed because no UDP ephemeral port was available.	User control of Ephmeral Port Ranges

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetGlobalStats (continued)	NWMTCPSTSMCRCfg Existing TCP stats changed: NWMTCPSTCurrEstab NWMTCPSTActiveOpened NWMTCPSTPassiveOpened NWMTCPSTConnClosed NWMTCPSTInSegs NWMTCPSTOutSegs NWMTCPSTOutRsts NWMTCPSTEstabResets NWMTCPSTAcceptCount NWMTCPSTKeepAliveProbes NWMTCPSTKeepAliveDrop NWMTCPSTFinwait2Drops New SMC-R stats: NWMTCPSTSMCRCurrEstabLnks NWMTCPSTSMCRLnkActTimeOut NWMTCPSTSMCRActLnkOpened NWMTCPSTSMCRPasLnkOpened NWMTCPSTSMCRLnksClosed NWMTCPSTSMCRCurrEstab NWMTCPSTSMCRActiveOpened NWMTCPSTSMCRPassiveOpened NWMTCPSTSMCRConnClosed NWMTCPSTSMCRInSegs NWMTCPSTSMCROutSegs NWMTCPSTSMCRInRsts NWMTCPSTSMCROutRsts	V2R1	• New flag bit NWMTCPSTSMCRCfg is set in the NWMTCPSTFlags field to indicate whether the SMCR parameter is configured on the GLOBALCONFIG statement. • When the SMCR parameter is configured on the GLOBALCONFIG statement, the listed TCP counters reflect all TCP connections, including connections over SMC-R links. • The listed SMC-R statistics are added.	Shared Memory Communications over Remote Direct Memory Access
	NWMTCPSTConnFloods	V1R13	New field defined - The number of TCP servers under a potential connection flood attack.	Expanded Intrusion Detection Services
	NWMTCPSTConnStalls	V1R13	New field defined -The number of TCP connections whose send data flow is stalled.	Expanded Intrusion Detection Services
GetIfs	• NWMIfFlags – NWMIfPNetIDFlg • NWMIfFlags2 – NWMIfSMCDFlg – NWMIfIsmAssoc • NWMIfType • NWMIfAssocName • NWMIfPFID • NWMIfSMCRStatus • NWMIfSMCDStatus • NWMIfGID • NWMIfPNetID	V2R2	• New NWMIfSMCDFlg flag bit is set in the NWMIfFlags2 field for OSD and HiperSockets interfaces that have SMCD specified on the INTERFACE statement. • New NWMIfIsmAssoc is set in the NWMIfFlags2 field to indicate that this ISM is associated with an OSD or HiperSockets interface. • Listed fields are updated to include information for SMC-D. • The NWMIFSMCRVLAN value is obsolete from the NWMIfSMCRStatus field.	Shared Memory Communications - Direct Memory Access
	NWMIfFlags	V2R1	• The NWMIfDefIntf flag bit is set in the NWMIfFlags field for IPv4 IPAQIDIO and VIRTUAL interfaces that are defined by the INTERFACE statement. • The NWMIfBcast flag bit is set in the NWMIfFlags field for IPv4 IPAQIDIO interfaces defined by the INTERFACE statement with the IPBCAST parameter specified.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetIfs (continued)	NWMIfRouteMask	V2R1	The NWMIfRouteMask provides the configured subnet mask for IPv4 IPAQIDIO interfaces defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NWMIfChpID	V2R1	The NWMIfChpID provides the CHPID value for IPv4 IPAQIDIO interfaces defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NWMIfCfgMtu	V2R1	The NWMIfCfgMtu provides the configured MTU value for IPv4 IPAQIDIO interfaces defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NWMIfDatapathNum	V2R1	The NWMIfDatapathNum provides the datapath address for IPv4 IPAQIDIO interfaces defined by the INTERFACE statement, and for IPv6 IPAQIDIO6 interfaces.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NWMIfAssocName	V2R1	The NWMIfAssocName provides the TRLE name for IPv4 IPAQIDIO interfaces defined by the INTERFACE statement, and for IPv6 IPAQIDIO6 interfaces.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NWMIfSrcVipaIntfName	V2R1	The NWMIfSrcVipaIntfName provides the SOURCEVIPAINTERFACE name for IPv4 IPAQIDIO interfaces defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NWMIpadAddr	V2R1	The NWMIpadAddr provides the IP address for IPv4 IPAQIDIO and VIRTUAL interfaces defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NWMIfFlags	V2R1	• The NWMIfSMCRFlg flag bit is set in the NWMIfFlags field for OSD interfaces that have SMCR specified on the INTERFACE statement • The NWMIfPNetIDFlg flag bit is set in the NWMIfFlags field for OSD, OSX and RNIC interfaces to indicate the NWMIfPNetID field contains the Physical network ID.	Shared Memory Communications over Remote Direct Memory Access
	NWMIfType	V2R1	The NWMIfType field can have a new NWMIFTRNIC type for 10GbE RoCE Express interfaces, which are represented as RNIC interfaces.	Shared Memory Communications over Remote Direct Memory Access
	NWMIfMacAddr	V2R1	The NWMIfMacAddr field contains the VMAC address generated by the VTAM DLC layer for 10GbE RoCE Express interfaces.	Shared Memory Communications over Remote Direct Memory Access
	NWMIfAssocName	V2R1	The NWMIfAssocName field contains the TRLE name for 10GbE RoCE Express interfaces.	Shared Memory Communications over Remote Direct Memory Access

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetIfs (continued)	NWMIfPFID	V2R1	The new NWMIfPFID field contains the PFID for 10GbE RoCE Express interfaces.	Shared Memory Communications over Remote Direct Memory Access
	NWMIfGID	V2R1	The new NWMIfGID field contains the GID for 10GbE RoCE Express interfaces.	Shared Memory Communications over Remote Direct Memory Access
	NWMIfSMCRStatus	V2R1	The new NWMIfSMCRStatus field contains the SMCR status for OSD interfaces.	Shared Memory Communications over Remote Direct Memory Access
	NWMIfPNetID	V2R1	The new NWMIfPNetID field contains the Physical network ID for active OSD, OSX and 10GbE RoCE Express interfaces.	Shared Memory Communications over Remote Direct Memory Access
	NWMIfFlags2	V2R1	The NWMIfRnicAssoc is set in the NWMIfFlags2 field to indicate that this 10GbE RoCE Express interface is associated with an OSD interface.	Shared Memory Communications over Remote Direct Memory Access
	NWMIfChksumOffload and NWMIfTcpSegOffload parameters	V1R13	These flags are now valid for IPAQENET6 interfaces.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NWMIFTHIPERIQDX	V1R13	New interface type for IQDX (for interface types of either IPAQIQX or IPAQIQX6).	HiperSockets optimization for intraensemble data networks
	NWMIfIQDXFlg	V1R13	For an OSX interface, an indicator if an associated dynamic IQDX interface name field is provided.	HiperSockets optimization for intraensemble data networks
	NWMIfIQDXName	V1R13	For an OSX interface, the associated dynamic IQDX interface name.	HiperSockets optimization for intraensemble data networks
GetIfStats	NWMIFTHIPERIQDX	V1R13	New interface type for IQDX (for interface types of either IPAQIQX or IPAQIQX6).	HiperSockets optimization for intraensemble data networks
	NWMIfStIQDXFlg	V1R13	For an OSX interface, an indicator if statistics for an associated dynamic IQDX interface exists.	HiperSockets optimization for intraensemble data networks
	NWMIfStInIQDXBytes NWMIfStInIQDXUcastPkts NWMIfStOutIQDXBytes NWMIfStOutIQDXUcastPkts	V1R13	For an OSX interface, statistics for bytes and unicast packets sent and received over the associated dynamic IQDX interface.	HiperSockets optimization for intraensemble data networks
GetIfStatsExtended	NWMIFTHIPERIQDX	V1R13	New interface type for IQDX (for interface types of either IPAQIQDX or IPAQIQDX6)	HiperSockets optimization for intraensemble data networks
GetIsms	N/A	V2R2	New poll-type request that obtains information for ISM interfaces.	Shared Memory Communications - Direct Memory Access

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetProfile	IPv4 configuration section: NMTP_V4CFDynXcfSMCD	V2R2	New NMTP_V4CFDynXcfSMCD value that indicates whether the dynamically generated XCF interface can be used for new TCP connections with SMC-D.	Shared Memory Communications - Direct Memory Access
	IPv6 configuration section: NMTP_V6CFDynXcfSMCD	V2R2	New NMTP_V6CFDynXcfSMCD value that indicates whether the dynamically generated XCF interface can be used for new TCP connections with SMC-D.	Shared Memory Communications - Direct Memory Access
	Global configuration section: NMTP_GBCFFlags - NMTP_GBCFSMCD NMTP_GBCFFixedMemoryD NMTP_GBCFTcpKeepMinIntD	V2R2	• New NMTP_GBCFSMCD flag bit is set in the NMTP_GBCFFlags field to indicate that the SMCD operand was specified on the GLOBALCONFIG statement. • New NMTP_GBCFFixedMemoryD field that specifies the SMCD FIXEDMEMORY value. FIXEDMEMORY is specified in megabyte increments. • New NMTP_GBCFTcpKeepMinIntD field that specifies the SMCD TCPKEEPMININTERVAL value.	Shared Memory Communications - Direct Memory Access
	Interface section: NMTP_INTFFlags - NMTP_INTFSMCD	V2R2	New NMTP_INTFSMCD flag bit is set in the NMTP_INTFFlags field for OSD and HiperSockets interfaces that have SMCD specified or that take the SMCD default on the INTERFACE statement.	Shared Memory Communications - Direct Memory Access
	NMTP_GBCFAdjDVMSS	V2R2	Provides the value of the GLOBLACONFIG ADJUSTDVIPAMSS parameter.	VIPAROUTE fragmentation avoidance
	NMTP_GBCFSMCGFlags	V2R2	New flag byte field NMTP_GBCFSMCGFlags with the following flag bits: • NMTP_GBCFAutoCache • NMTP_GBCFAutoSMC	• Shared Memory Communications over RDMA enhancements • Shared Memory Communications - Direct Memory Access
	NMTP_IPSecRule	V2R2	New flags and fields to support the new and modified parameters on the IPSECRULE and IPSEC6RULE profile statements.	TCPIP profile IP security filter enhancements
	NMTP_PORTRsvOptions	V2R2	• New flag bit NMTP_PORTRSMC that indicates this port or port range is enabled for SMC-R and SMC-D. • New flag bit NMTP_PORTRNoSMC that indicates this port or port range is disabled for SMC-R and SMC-D.	• Shared Memory Communications over RDMA enhancements • Shared Memory Communications - Direct Memory Access
	NMTP_TCCFFlags	V2R2	New flag NMTP_TCCFAutoDelayAcks that indicates the setting of TCPCONFIG AUTODELAYACKS.	TCP Autonomic Tuning
	NMTP_PIDSEye	V2R1	In the C header file, EZBNMMPC, eyecatcher constant, NMTP_PIDSEYEC has been corrected.	Release update
	NMTP_V6CFDynXcfAddr	V2R1	In the C header file, EZBNMMPC, this IPv6 address field has been redefined from char to struct in6_addr.	Release update
	NMTP_IPA6Addr	V2R1	In the C header file, EZBNMMPC, this IPv6 address field has been redefined from char to struct in6_addr.	Release update

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetProfile (continued)	NMTP_INTFFlags	V2R1	New flag NMTP_INTFTempIP in field NMTP_INTFFlags that indicates the Interface is configured with the TEMPIP parameter.	Enable DHCP clients on OSA Interfaces
	NMTP_TCCFConnectTimeOut NMTP_TCCFConnectInitInterval NMTP_TCCFFRRThreshold NMTP_TCCFKeepAliveProbes NMTP_TCCFKAProbeInterval NMTP_TCCFMaxRetransmit NMTP_TCCFNagle NMTP_TCCFQueuedRTT NMTP_TCCFRetransmitAttempts NMTP_TCCFMaxSndBufSize NMTP_TCCFTimeWaitInterval	V2R1	New fields that indicates the setting of new TCPCONFIG parameters: • CONNECTTIMEOUT • CONNECTINITINTERVAL • FRRTHRESHOLD • KEEPALIVEPROBES • KEEPALIVEPROBEINTERVAL • MAXIMUMRETRANSMITTIME • NAGLE and NONAGLE • QUEUEDRTT • RETRANSMITATTEMPTS • TCPMAXSENDBUFRSIZE • TIMEWAITINTERVAL	Enhanced TCP protocol configuration options and default settings
	NMTP_GBCFFlags NMTP_GBCFPFidCnt NMTP_GBCFFixedMemory NMTP_GBCFTcpKeepMinInt NMTP_GBCFPFs array	V2R1	• The new NMTP_GBCFSMCR flag bit is set in the NMTP_GBCFFlags field to indicate that the SMCR operand was specified on the GLOBALCONFIG statement. • The new NMTP_GBCFPFidCnt field indicates the current number of configured PCI-function ID (PFID) and Port number entries in the NMTP_GBCFPFs array. • The new NMTP_GBCFFixedMemory field specifies the SMCR FIXEDMEMORY value. FIXEDMEMORY is specified in megabyte increments. • The new NMTP_GBCFTcpKeepMinInt field specifies the SMCR TCPKEEPMININTERVAL value. • The new NMTP_GBCFPFs array contains a maximum of 16 PFID and port number paired entries: – NMTP_GBCFPFid is the 2-byte hexadecimal PFID value. – NMTP-GBCFPFport is the 1-byte decimal port number. – NMTP_GBCFPFmtu is a 2-byte decimal maximum transmission unit (MTU) value.	Shared Memory Communications over Remote Direct Memory Access

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetProfile (continued)	NMTP_PORTFlags	V2R1	The NMTP_PORTRNoSMCR flag bit is set in the NMTP_PORTFlags field to indicate this port or port range is disabled for SMC-R.	Shared Memory Communications over Remote Direct Memory Access
	NMTP_INTFFlags	V2R1	The NMTP_INTFSMCR flag bit is set in the NMTP_INTFFlags field for OSA interfaces that have SMCR specified or that take the SMCR default on the INTERFACE statement.	Shared Memory Communications over Remote Direct Memory Access
	NMTP_MGMTSmf119Types	V2R1	• The new NMTP_MGMT119SmcrGrpStats flag bit is set in the NMTP_MGMTSmf119Type field to indicate that the new SMC-R link group statistics records were requested on the SMFCONFIG profile statement. • The new NMTP_MGMT119SmcrLnkEvent flag bit is set in the NMTP_MGMTSmf119Type field to indicate that the new SMC-R link state start and end records were requested on the SMFCONFIG profile statement.	Shared Memory Communications over Remote Direct Memory Access
	NMTP_V4CFFlags	V2R1	The description of flag NMTP_V4CFQDIOAcc is updated. The restriction of the QDIO Accelerator to sysplex distributor traffic is no longer determined only by whether IP datagram forwarding is enabled.	QDIO acceleration coexistence with IP filtering
	NMTP_TCCFSelectiveACK	V2R1	New flag is added to indicate the setting of TCPCONFIG SELECTIVEACK.	TCP support for selective acknowledgements
	NMTP_NETACache	V2R1	New field is added to indicate the setting of the CACHEALL, CACHEPERMIT, and CACHESAME parameters on the NETACCESS statement.	Improve auditing of NetAccess rules
	NMTP_TCCFEphemPortLow	V2R1	New field is added to indicate the low and high port values for TCP ephemeral ports.	User control of Ephmeral Port Ranges
	NMTP_TCCFEphPortHighNum	V2R1	New fields is added to indicate the low and high port values for TCP ephemeral ports.	User control of Ephmeral Port Ranges
	NMTP_UDCFEphemPortLow	V2R1	New fields is added to indicate the low and high port values for UDP ephemeral ports	User control of Ephmeral Port Ranges
	NMTP_UDCFEphPortHighNum	V2R1	New fields is added to indicate the low and high port values for UDP ephemeral ports	User control of Ephmeral Port Ranges

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetProfile (continued)	NMTP_V4CFDynXcfSrcVipaIfNameFlg	V2R1	New flag is added to indicate if the dynamic XCF source VIPA interface name is specified.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NMTP_V4CFDynXcfSrcVipaIfName	V2R1	New field is added to indicate the configured dynamic XCF source VIPA interface name.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NMTP_INTFDefIntf NMTP_INTFFlags	V2R1	The NMTP_INTFDefIntf flag bit is set in the NMTP_INTFFlags field for IPv4 IPAQIDIO and VIRTUAL interfaces that are defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NMTP_INTFIpBcast	V2R1	The NMTP_INTFIpBcast flag bit is set in the NMTP_INTFFlags field for IPv4 IPAQIDIO interfaces that are defined by the INTERFACE statement with the IPBCAST parameter specified.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NMTP_INTFChpID	V2R1	The NMTP_INTFChpID provides the CHPID value for IPv4 IPAQIDIO interfaces that are defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NMTP_INTFIPv4Mask	V2R1	The NMTP_INTFIPv4Mask provides the configured subnet mask for IPv4 IPAQIDIO interfaces that are defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NMTP_INTFMtu	V2R1	The NMTP_INTFMtu provides the configured MTU value for IPv4 IPAQIDIO interfaces that are defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NMTP_INTFIPv4Addr	V2R1	The NMTP_INTFIPv4Addr provides the IP address for IPv4 IPAQIDIO and VIRTUAL interfaces that are defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NMTP_INTFSrcVipaIntfName	V2R1	The NMTP_INTFSrcVipaIntfName provides the SOURCEVIPAINTERFACE name for IPv4 IPAQIDIO interfaces that are defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NMTP_GBCFSegOffload	V1R13	Use of this flag is deprecated. Use NMTP_V4CFSegOffload.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NMTP_V4CFChkOffload	V1R13	New flag that indicates setting of IPCONFIG CHECKSUMOFFLOAD.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NMTP_V4CFSegOffload	V1R13	New flag that indicates setting of IPCONFIG SEGMENTATIONOFFLOAD.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NMTP_V6CFChkOffload	V1R13	New flag that indicates setting of IPCONFIG6 CHECKSUMOFFLOAD.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NMTP_V6CFSegOffload	V1R13	New flag that indicates setting of IPCONFIG6 SEGMENTATIONOFFLOAD.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NMTP_GBCFAutoIQDX	V1R13	New flags that indicates setting of GLOBALCONFIG AUTOIQDX	HiperSockets optimization for intraensemble data networks
GetProfile (continued)	NMTP_DVCFSAFNameSet	V1R13	New flag in field NMTP_DVCFFlags that indicates if the SAF parameter is specified on the VIPARANGE statement.	Improved security granularity for VIPARANGE DVIPAs
	NMTP_DVCFSAFName	V1R13	New field that indicates the name that is specified on the SAF parameter of the VIPARANGE statement.	Improved security granularity for VIPARANGE DVIPAs
	NMTP_PORTJobName	V1R13	This field can now contain a job name consisting of a 1-7 character prefix followed by an asterisk.	Wildcard support for the PORTRANGE statement

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetRnics	N/A	V2R1	New poll-type request to obtain information for SMC-R link groups and the SMC-R links in each group.	Shared Memory Communications over Remote Direct Memory Access
GetSmcDLinks	N/A	V2R2	New poll-type request to obtain information for SMC-D links.	Shared Memory Communications - Direct Memory Access
GetSmcLinks	N/A	V2R1	New poll-type request to obtain information for 10GbE RoCE Express interfaces.	Shared Memory Communications over Remote Direct Memory Access
GetStorageStatistics	• NWMStgFlags – NWMStgSMCDCfg • New SMC-D storage utilization – NWMStg64SMCDFixedCurrent – NWMStg64SMCDFixedMax – NWMStg64SMCDFixedLimit	V2R2	• New flag bit NWMStgSMCDCfg is set in the NWMStgFlags field to indicate whether the SMCD parameter is configured on the GLOBALCONFIG statement. • The SMC-D storage utilization information is added when the SMCD parameter is configured on the GLOBALCONFIG statement	Shared Memory Communications - Direct Memory Access
	NWMStgSMCRCfg New SMC-R storage utilization: NWMStg64SMCRFixedCurrent NWMStg64SMCRFixedMax NWMStg64SMCRFixedLimit NWMStg64SMCRSendCurrent NWMStg64SMCRSendMax NWMStg64SMCRRecvCurrent NWMStg64SMCRRecvMax	V2R1	• New flag bit NWMStgSMCRCfg is set in the NWMStgFlags field to indicate whether the SMCR parameter is configured on the GLOBALCONFIG statement. • The SMC-R storage utilization information is added when the SMCR parameter is configured on the GLOBALCONFIG statement.	Shared Memory Communications over Remote Direct Memory Access
	NWMStg64PrivateCurrent NWMStg64PrivateMax NWMStg64PrivateFree NWMStg64PrivateTrace NWMStg64ComTrace	V1R13	New parameters to return the storage usage information for 64-bit private storage and 64-bit storage used for tracing.	Increased CTRACE and VIT capacity

Table 28. Summary of new Communications Server TCP/IP callable NMI (EZBNMIFR) (continued)

Request	Parameter/output	Rel.	Description	Reason for change
GetTCPListeners	• NWMTCPLSmcdCfg • NWMTCPLSmcdCurrConn • NWMTCPLSmcdTotalConn	V2R2	• New NWMTCPLSmcdCfg flag set in the NWMTCPLSmcFlags field that indicates whether the SMC-D processing is or has been in effect. • New field NWMTCPLSmcdCurrConn that indicates the number of active connections to this server that use SMC-D. • New field NWMTCPLSmcdTotalConn that indicates the number of connections that this server has accepted using SMC-D.	Shared Memory Communications - Direct Memory Access
	NWMTCPLSmcAutoPct	V2R2	New field NWMTCPLSmcAutoPct that indicates percentage of connections that request SMC-R whose workload pattern matched SMC-R criteria during the last AutoSMCR function interval.	Shared Memory Communications over RDMA enhancements
	NWMTCPLSmcCurrConn	V2R2	New field NWMTCPLSmcCurrConn that indicates the number of active connections to this server that use SMC-R.	Shared Memory Communications over RDMA enhancements
	NWMTCPLSmcFlags	V2R2	New flag byte NWMTCPLSmcFlags with the following flag bits: • NWMTCPLSmcrCfg • NWMTCPLSmcAutoSMC • NWMTCPLSmcUseSMCR • NWMTCPLSmcCfgPort	Shared Memory Communications over RDMA enhancements
	NWMTCPLSmcTotalConn	V2R2	New field NWMTCPLSmcTotalConn that indicates the number of connections that this server has accepted using SMC-R.	Shared Memory Communications over RDMA enhancements
	NWMTCPLConnFlood	V1R13	New bit defined that indicates whether the server is under a potential connection flood attack.	Expanded Intrusion Detection Services
GetTnProfile	SMF119TN_HGHName	V2R2	In the C header, ezasmf.h, the length of this field was changed from zero to the maximum length of 255, in order to resolve a compiler warning message.	Release update
	SMF119TN_TPSSLV3	V2R1	New field to enable or disable SSLV3	APAR PI28679

TCPIPCS subcommand

Table 29 lists the TCPIPCS subcommand options.

The TCPIPCS command contains the OPTLOCAL specification in some displays.

Table 29. Summary of new and changed Communications Server TCPIPCS subcommand

Option	Release	Description	Reason for change
CONFIG	V2R2	Supports new ISM interface type.	Shared Memory Communications - Direct Memory Access
	V2R1	Supports new RNIC interface type.	
	V1R13	Supports new IPAQIQDX and IPAQIQDX6 interface types.	HiperSockets optimization for intraensemble data networks
HASH	V2R1	Displays information about the structure of IPv6 dynamic VIPA shadow tunnel hash tables.	Sysplex-Wide Security Associations for IPv6

Table 29. Summary of new and changed Communications Server TCPIPCS subcommand (continued)

Option	Release	Description	Reason for change
IPSEC	V2R1	Displays information about IPv6 IP security shadow tunnels.	Sysplex-Wide Security Associations for IPv6
	V2R1	Includes log limit value of the filter in the formatted information.	Limit defensive filter logging
MAP	V2R1	Includes the storage that is used for the IPv6 policy-based route tables.	IPv6 support for policy-based routing
	V2R1	Displays storage usage information for IPv6 dynamic VIPA shadow tunnel hash tables.	Sysplex-Wide Security Associations for IPv6
POLICY	V2R1	IPv6 policy is included in the display of policy-based routing rules and actions.	IPv6 support for policy-based routing
PROFILE	Every release	Displays the current TCP/IP stack configuration from information in the dump by creating the profile statements that represent the configuration. See "PROFILE.TCPIP statement and parameter changes" on page 712 for information about the profile statement changes for a specific release.	Release update
ROUTE	V2R1	• When the PR parameter is used to display all search tree and update tree routes for all active policy-based route tables, IPv6 routes are included in the report. • When the PD parameter is used to display all search tree and update tree routes for all policy-based route tables that have been marked for deletion , IPv6 routes are included in the report.	IPv6 support for policy-based routing
STATE	V2R2	Supports new ISM interface type.	Shared Memory Communications - Direct Memory Access
	V2R1	Supports new RNIC interface type.	Shared Memory Communications over Remote Direct Memory Access
	V1R13	Supports new IPAQIQDX and IPAQIQDX6 interface types.	HiperSockets optimization for intraensemble data networks
TIMER	V2R1	For timers that are configured to do a cross-memory post, the target address space ASCB and ASID values are displayed.	Real-time application-controlled TCP/IP trace NMI
TRACE	V2R1	Displays each CTE header in a CTRACE buffer	Support for additional diagnostic information about Ctrace
	V2R1	New ALL and RCC subparameters are added. The RCC subparameter formats information about applications using the Real-time application-controlled TCP/IP trace NMI.	Real-time application-controlled TCP/IP trace NMI
TREE	V2R1	Includes the search and update trees for IPv6 policy-based route tables.	IPv6 support for policy-based routing
TTLS	V2R2	The report output can have a new value of RFC5280 for CertValidationMode.	AT-TLS certificate processing enhancements
	V2R2	When the CONN parameter is specified, the command displays values that pertain to certificate revocation lists (CRLs) for the new AT-TLS policy agent statements and parameters.	AT-TLS certificate processing enhancements
	V2R1	Displays new parameters on AT-TLS configuration statements.	AT-TLS support for TLS v1.2 and related features

Table 29. Summary of new and changed Communications Server TCPIPCS subcommand (continued)

Option	Release	Description	Reason for change
XCF	V1R13	Displays the dynamic VIPA that was created using the bind socket call, the SIOCSVIPA or SIOCSVIPA6 ioctl call, or the MODDVIPA utility, including the new SAF resource name if it is configured.	Improved security granularity for VIPARANGE DVIPAs

TCP/IP stack records

Table 30 lists the changes made to the TCP/IP stack SMF type 119 records.

Table 30. Summary of new and changed Communications Server SMF type 119 record - TCP/IP stack records

Record type	Record field	Release	Description	Reason for change
Interface statistics (subtype 6)	SMF119IS_IFDesc SMF119IS_IFFlags SMF119IS_IFPNetID	V2R1	• The SMF119IS_IFDesc field can have a new SMF119IS_IFLink_RNIC type for 10GbE RoCE Express interfaces, which are represented as RNIC interfaces. • New SMF119IS_IFFlags field contains information, related to the SMC-R characteristics, if any, for the reported interface. • New SMF119IS_IFPNetID field contains the Physical network ID for active OSD, OSX and RNIC interfaces.	Shared Memory Communications over Remote Direct Memory Access
	SMF119IS_IFLink_IPQIQDX SMF119IS_IFLink_IPQIQX6	V1R13	New interface types IPAQIQDX and IPAQIQDX6	HiperSockets optimization for intraensemble data networks
	SMF119IS_IfIQDXName SMF119IS_IfInIQDXBytes SMF119IS_IfInIQDXUniC SMF119IS_IfOutIQDXBytes SMF119IS_IfOutInIQDXUniC	V1R13	New fields to show the associated dynamic IQDX for an OSX interface and the number of bytes and unicast packets that traversed it.	HiperSockets optimization for intraensemble data networks

Table 30. Summary of new and changed Communications Server SMF type 119 record - TCP/IP stack records (continued)

Record type	Record field	Release	Description	Reason for change
TCP/IP profile record (subtype 4)	IPv4 configuration section • NMTP_V4CFDynXcfSMCD IPv6 configuration section • NMTP_V6CFDynXcfSMCD Global configuration section • NMTP_GBCFFlags – NMTP_GBCFSMCD • NMTP_GBCFFixedMemoryD • NMTP_GBCFTcpKeepMinIntD Interface section • NMTP_INTFFlags – NMTP_INTFSMCD	V2R2	IPv4 configuration section • The new NMTP_V4CFDynXcfSMCD value is specified whether the dynamically generated XCF interface can be used for new TCP connections with SMC-D. IPv6 configuration section • The new NMTP_V6CFDynXcfSMCD value is specified whether the dynamically generated XCF interface can be used for new TCP connections with SMC-D. Global configuration section: • The new NMTP_GBCFSMCD flag bit is set in the NMTP_GBCFFlags field to indicate that the SMCD operand was specified on the GLOBALCONFIG statement. • The new NMTP_GBCFFixedMemoryD field specifies the SMCD FIXEDMEMORY value. FIXEDMEMORY is specified in megabyte increments. • The new NMTP_GBCFTcpKeepMinIntD field specifies the SMCD TCPKEEPMININTERVAL value. Interface section: • The new NMTP_INTFSMCD flag bit is set in the NMTP_INTFFlags field for OSA or HiperSocket interfaces that have SMCD specified or that take the SMCD default on the INTERFACE statement.	Shared Memory Communications – Direct Memory Access
	NMTP_GBCFAdjDVMSS	V2R2	Provides the value of the GLOBLACONFIG ADJUSTDVIPAMSS parameter.	VIPAROUTE fragmentation avoidance
	NMTP_GBCFSMCGFlags	V2R2	New flag byte field NMTP_GBCFSMCGFlags with the following flag bits: • NMTP_GBCFAutoCache • NMTP_GBCFAutoSMC	• Shared Memory Communications over RDMA enhancements • Shared Memory Communications - Direct Memory Access
	NMTP_IPSecRule	V2R2	New flags and fields to support the new and modified parameters on the IPSECRULE and IPSEC6RULE profile statements.	TCPIP profile IP security filter enhancements
	NMTP_PORTRsvOptions	V2R2	New flag bits NMTP_PORTRSMC and NMTP_PORTRNoSMC in field NMTP_PORTRsvOptions.	• Shared Memory Communications over RDMA enhancements • Shared Memory Communications - Direct Memory Access
	NMTP_TCCFFlags	V2R2	New flag NMTP_TCCFAutoDelayAcks that indicates the setting of TCPCONFIG AUTODELAYACKS.	TCP Autonomic Tuning

Table 30. Summary of new and changed Communications Server SMF type 119 record - TCP/IP stack records (continued)

Record type	Record field	Release	Description	Reason for change
TCP/IP profile record (subtype 4) (continued)	NMTP_INTFFlags	V2R1	New flag NMTP_INTFTempIP in field NMTP_INTFFlags that indicates the Interface is configured with the TEMPIP parameter.	Enable DHCP clients on OSA Interfaces
	NMTP_TCCFTimeWaitInterval	V2R1	New field that provides the setting of the TCPCONFIG TIMEWAITINTERVAL value.	Enhanced TCP protocol configuration options and default settings
	NMTP_TCCFRetransmitAttempts	V2R1	New field that provides the setting of the TCPCONFIG RETRANSMITATTEMPTS value.	Enhanced TCP protocol configuration options and default settings
	NMTP_TCCFConnectTimeOut	V2R1	New field that provides the setting of the TCPCONFIG CONNECTTIMEOUT value.	Enhanced TCP protocol configuration options and default settings
	NMTP_TCCFConnectInitInterval	V2R1	New field that provides the setting of the TCPCONFIG CONNECTINITINTERVAL value.	Enhanced TCP protocol configuration options and default settings
	NMTP_TCCFNagle	V2R1	New field that provides the setting of the TCPCONFIG NAGLE value.	Enhanced TCP protocol configuration options and default settings
	NMTP_TCCFKeepAliveProbes	V2R1	New field that provides the setting of the TCPCONFIG KEEPALIVEPROBES value.	Enhanced TCP protocol configuration options and default settings
	NMTP_TCCFKAProbeInterval	V2R1	New field that provides the setting of the TCPCONFIG KEEPALIVEPROBEINTERVAL value.	Enhanced TCP protocol configuration options and default settings
	NMTP_TCCFQueuedRTT	V2R1	New field that provides the setting of the TCPCONFIG QUEUEDRTT value.	Enhanced TCP protocol configuration options and default settings
	NMTP_TCCFFRRThreshold	V2R1	New field that provides the setting of the TCPCONFIG FRRTHRESHOLD value.	Enhanced TCP protocol configuration options and default settings
	NMTP_TCCFSelectiveACK	V2R1	New flag to indicate the setting of SELECTIVEACK/NOSELECTIVEACK.	TCP support for selective acknowledgments
	NMTP_TCCFDefltMaxSndBufSize	V2R1	New field that provides the setting of the TCPCONFIG TCPMAXSENDBUFRSIZE value.	Enhanced TCP protocol configuration options and default settings

Table 30. Summary of new and changed Communications Server SMF type 119 record - TCP/IP stack records (continued)

Record type	Record field	Release	Description	Reason for change
TCP/IP profile record (subtype 4) (continued)	NMTP_TCCFEphemPortBegNum	V2R1	The NMTP_TCCFEphemPortBegNum field contains the beginning port range value for TCP ephemeral ports.	User control of Ephmeral Port Ranges
	NMTP_TCCFEphemPortEndNum	V2R1	The NMTP_TCCFEphemPortEndNum field contains the ending port range value for TCP ephemeral ports.	User control of Ephmeral Port Ranges
	NMTP_UDCFEphemPortBegNum	V2R1	The NMTP_UDCFEphemPortBegNum field contains the beginning port range value for UDP ephemeral ports.	User control of Ephmeral Port Ranges
	NMTP_UDCFEphemPortEndNum	V2R1	The NMTP_UDCFEphemPortEndNumfield contains the ending port range value for UDP ephemeral ports.	User control of Ephmeral Port Ranges
	NMTP_V4CFDynXcfSrcVipaIfNameFlg	V2R1	New flag is added to indicate if the dynamic XCF source VIPA interface name is specified.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	NMTP_V4CFDynXcfSrcVipaIfName	V2R1	New field is added to provide the configured dynamic XCF source VIPA interface name	IPv4 INTERFACE statement for HiperSockets and Static VIPAs
	• NMTP_INTFFlags • NMTP_INTFChpID • NMTP_INTFIPv4MaskNMTP_INTFMtu • NMTP_INTFSrcVipaIntfName	V2R1	• The NMTP_INTFDefIntf bit is set in the NMTP_INTFFlags field for IPv4 IPAQIDIO and VIRTUAL interfaces that are defined by the INTERFACE statement. • The NMTP_INTFIpBcast is set in the NMTP_INTFFlags field for IPv4 IPAQIDIO interfaces that are defined by the INTERFACE statement with the IPBCAST parameter specified. • The NMTP_INTFChpID provides the CHPID value for IPv4 IPAQIDIO interfaces that are defined by the INTERFACE statement. • The NMTP_INTFIPv4Mask provides the configured subnet mask for IPv4 IPAQIDIO interfaces that are defined by the INTERFACE statement. • The NMTP_INTFMtu provides the configured MTU value for IPv4 IPAQIDIO interfaces that are defined by the INTERFACE statement. • The NMTP_INTFSrcVipaIntfName provides the SOURCEVIPAINTERFACE name for IPv4 IPAQIDIO interfaces that are defined by the INTERFACE statement.	IPv4 INTERFACE statement for HiperSockets and Static VIPAs

Table 30. Summary of new and changed Communications Server SMF type 119 record - TCP/IP stack records (continued)

Record type	Record field	Release	Description	Reason for change
TCP/IP profile record (subtype 4) (continued)	NMTP_NETACache	V2R1	New field is added to indicate the setting of the CACHEALL, CACHEPERMIT, and CACHESAME parameters on the NETACCESS statement.	Improve auditing of NetAccess rules
	NMTP_TCCFSelectiveACK	V2R1	New flag is added to indicate the setting of SELECTIVEACK/NOSELECTIVEACK.	TCP support for selective acknowledgements
	NMTP_V4CFFlags	V2R1	The description of flag NMTP_V4CFQDIOAcc is updated. The restriction of QDIO Accelerator to sysplex distributor traffic is no longer determined only by whether IP datagram forwarding is enabled.	QDIO acceleration coexistence with IP filtering
	NMTP_GBCFFlags NMTP_GBCFPFidCnt NMTP_GBCFFixedMemory NMTP_GBCFTcpKeepMinInt NMTP_GBCFPFs array	V2R1	• The new NMTP_GBCFSMCR flag bit is set in the NMTP_GBCFFlags field to indicate that the SMCR operand was specified on the GLOBALCONFIG statement. • The new NMTP_GBCFPFidCnt field indicates the current number of configured PCI-function ID (PFID) and Port number entries in the NMTP_GBCFPFs array. • The new NMTP_GBCFFixedMemory field specifies the SMCR FIXEDMEMORY value. FIXEDMEMORY is specified in megabyte increments. • The new NMTP_GBCFTcpKeepMinInt field specifies the SMCR TCPKEEPMININTERVAL value. • The new NMTP_GBCFPFs array contains a maximum of 16 PFID and port number paired entries: – NMTP_GBCFPFid is the 2-byte hexadecimal PFID. – NMTP_GBCFPFport is the 1-byte decimal port number. – NMTP_GBCFPFmtu is a 2-byte maximum transmission unit (MTU) decimal value.	Shared Memory Communications over Remote Direct Memory Access
	NMTP_PORTFlags	V2R1	The NMTP_PORTRNoSMCR flag bit is set in the NMTP_PORTFlags field to indicate this port or port range is disabled for SMC-R.	Shared Memory Communications over Remote Direct Memory Access
	NMTP_INTFFlags	V2R1	The NMTP_INTFSMCR flag bit is set in the NMTP_INTFFlags field for OSA interfaces that have SMCR specified or that take the SMCR default on the INTERFACE statement.	Shared Memory Communications over Remote Direct Memory Access
	NMTP_MGMTSmf119Types	V2R1	• The new NMTP_MGMT119SmcrGrpStats flag bit is set in the NMTP_MGMTSmf119Type field to indicate that the new SMC-R link group statistics records were requested on the SMFCONFIG profile statement. • The new NMTP_MGMT119SmcrLnkEvent flag bit is set in the NMTP_MGMTSmf119Type field to indicate that the new SMC-R link state start and end records were requested on the SMFCONFIG profile statement.	Shared Memory Communications over Remote Direct Memory Access

Table 30. Summary of new and changed Communications Server SMF type 119 record - TCP/IP stack records (continued)

Record type	Record field	Release	Description	Reason for change
TCP/IP profile record (subtype 4) (continued)	NMTP_PIDSEye	V2R1	In the C header file, EZBNMMPC, eyecatcher constant, NMTP_PIDSEYEC has been corrected.	Release update
	NMTP_V6CFDynXcfAddr	V2R1	In the C header file, EZBNMMPC, this IPv6 address field has been redefined from char to struct in6_addr.	Release update
	NMTP_IPA6Addr	V2R1	In the C header file, EZBNMMPC, this IPv6 address field has been redefined from char to struct in6_addr.	Release update
	NMTP_GBCFAutoIQDX	V1R13	Subtype 4. New flags to indicate setting of GLOBALCONFIG AUTOIQDX.	HiperSockets optimization for intraensemble data networks
	NMTP_GBCFSegOffload	V1R13	Use of this flag is deprecated. See NMTP_V4CFSegOffload.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NMTP_V4CFChkOffload	V1R13	New flag to indicate setting of IPCONFIG CHECKSUMOFFLOAD.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NMTP_V4CFSegOffload	V1R13	New flag to indicate setting of IPCONFIG SEGMENTATIONOFFLOAD.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NMTP_V6CFChkOffload	V1R13	New flag to indicate setting of IPCONFIG6 CHECKSUMOFFLOAD.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NMTP_V6CFSegOffload	V1R13	New flag to indicate setting of IPCONFIG6 SEGMENTATIONOFFLOAD.	OSA-Express4S QDIO IPv6 checksum and segmentation offload
	NMTP_DVCFSAFNameSet	V1R13	New flag in field NMTP_DVCFFlags to indicate if the SAF parameter is specified on the VIPARANGE statement.	Improved security granularity for VIPARANGE DVIPAs
	NMTP_DVCFSAFName	V1R13	New field to indicate the name specified on the SAF parameter of the VIPARANGE statement.	Improved security granularity for VIPARANGE DVIPAs
	NMTP_PORTJobName	V1R13	This field can now contain a job name prefix (1-7 character job name followed by an asterisk) for entries that represent a PORTRANGE profile statement.	Wildcard support for the PORTRANGE statement

Table 30. Summary of new and changed Communications Server SMF type 119 record - TCP/IP stack records (continued)

Record type	Record field	Release	Description	Reason for change
TCP/IP statistics record (subtype 5)	SMF119AP_TSTCEphPortExh	V2R1	SMF119AP_TSTCEphPortExh contains the interval count of number of bind() failures because no TCP ephemeral ports were available.	User control of Ephmeral Port Ranges
	SMF119AP_TSTCEphPortAvail	V2R1	SMF119AP_TSTCEphPortAvail contains the total number of TCP ephemeral ports that are available to use for bind() requests	User control of Ephmeral Port Ranges
	SMF119AP_TSTCEphPortInUse	V2R1	SMF119AP_TSTCEphPortInUse contains the current number of TCP ephemeral ports in use	User control of Ephmeral Port Ranges
	SMF119AP_TSTCEphPortMxUse	V2R1	SMF119AP_TSTCEphPortMxUse contains the maximum number of TCP ephemeral ports used	User control of Ephmeral Port Ranges
	SMF119AP_TSUDEphPortExh	V2R1	SMF119AP_TSUDEphPortExh contains the interval count of number of bind() failures because no UDP ephemeral ports were available.	User control of Ephmeral Port Ranges
	SMF119AP_TSUDEphPortAvail	V2R1	SMF119AP_TSUDEphPortAvail contains the total number of UDP ephemeral ports that are available to use for bind() requests.	User control of Ephmeral Port Ranges
	SMF119AP_TSUDEphPortInUse	V2R1	SMF119AP_TSUDEphPortInUse contains the current number of UDP ephemeral ports in use.	User control of Ephmeral Port Ranges
	SMF119AP_TSUDEphPortMxUse	V2R1	SMF119AP_TSUDEphPortMxUse contains the maximum number of UDP ephemeral ports used	User control of Ephmeral Port Ranges
	Existing TCP stats changed: SMF119AP_TSTCEstab SMF119AP_TSTCOpenConn SMF119AP_TSTCPassConn SMF119AP_TSTCConCls SMF119AP_TSTCInSegs SMF119AP_TSTCOSegs SMF119AP_TSTCReset SMF119AP_TSTCConReset SMF119AP_TSTCOKApr SMF119AP_TSTCDropKA SMF119AP_TSTCDropF2 New SMC-R stats: SMF119AP_TSSMCRCurrEstabLnks SMF119AP_TSSMCRLnkActTimeOut SMF119AP_TSSMCRActLnkOpened SMF119AP_TSSMCRPasLnkOpened SMF119AP_TSSMCRLnksClosed SMF119AP_TSSMCRCurrEstab SMF119AP_TSSMCRActiveOpened SMF119AP_TSSMCRPassiveOpened SMF119AP_TSSMCRConnClosed SMF119AP_TSTSMCRInSegs SMF119AP_TSTSMCROutSegs SMF119AP_TSSMCRInRsts SMF119AP_TSSMCROutRsts New SMC-R storage stats: SMF119AP_TSSTSMCRFixedCurrent SMF119AP_TSSTSMCRFixedMax SMF119AP_TSSTSMCRSendCurrent SMF119AP_TSSTSMCRSendMax SMF119AP_TSSTSMCRRecvCurrent SMF119AP_TSSTSMCRRecvMax	V2R1	• When the SMCR parameter is configured on the GLOBALCONFIG statement, the listed TCP counters reflect all TCP connections, including connections over SMC-R links. • The listed SMC-R stats are added at the end of the TCP statistics section. • The listed SMC-R storage stats are added in the storage statistics section.	Shared Memory Communications over Remote Direct Memory Access

Communications Server SNA summary of interface changes

This topic describes the updates to the following Communications Server SNA interfaces:

- Start options
- "Start option behavior changes"
- Definition statements
- "Commands"
- "Command behavior changes" on page 769
- "VTAM internal trace entries" on page 772
- VTAMMAP Formatted Dump changes
- Tuning statistics reports

Start option behavior changes

Table 31 lists the SNA start options that have changed behavior.

For complete information about all SNA start options, refer to *z/OS Communications Server: SNA Resource Definition Reference*.

Table 31. Summary of new and changed Communications Server start option behavior changes

Start option with changed behavior	Release	Description of update	Reason for change
AIMON	V2R2	The AIMON start option is enhanced to enable VTAM to monitor overdue adapter interrupts for internal shared memory (ISM) interfaces that are associated with Shared Memory Communications – Direct Memory Access (SMC-D) and OSA-Express QDIO interfaces.	Shared Memory Communications - Direct Memory Access
INOPDUMP	V2R2	New INOPDUMP control groups enable more granular control on which resources are eligible to initiate inoperative diagnostic dumps.	Shared Memory Communications - Direct Memory Access
TNSTAT	V2R2	The TNSTAT start option has no effect on a TRLE that represents an ISM device.	Shared Memory Communications - Direct Memory Access
TRACE	V1R13	The VIT operand DSPSIZE is no longer supported. Coding the DSPSIZE operand results in message IST448I DSPSIZE OPTION IGNORED - NO LONGER SUPPORTED.	Increased CTRACE and VIT capacity
	V1R13	The VIT operand SIZE specifies the number of megabytes of HVCOMMON storage to be used for the VIT table. Previously, it specified the number of pages of ECSA to be used for the VIT table. If you do not specify M (for megabyte), a default of 4M is used.	Increased CTRACE and VIT capacity

Commands

Table 32 lists the new and changed SNA commands.

For complete information about SNA commands, refer to the *z/OS Communications Server: SNA Operation*.

Table 32. Summary of new and changed Communications Server commands

Command	Release	Description	Reason for change
DISPLAY EE	V2R1	Added a new CPNAME filter.	Serviceability Enhancements

Table 32. Summary of new and changed Communications Server commands (continued)

Command	Release	Description	Reason for change
DISPLAY TRL	V2R2	A new value is defined for the CONTROL parameter. Specifying CONTROL=ISM displays all the internal shared memory (ISM) TRLEs.	Shared Memory Communications - Direct Memory Access
	V2R1	If the TRLE represents an OSA-Express in QDIO mode or in Hipersockets device, the display includes an additional message (IST2386I).	QDIO outbound flood prevention
	V2R1	A new value is defined for the CONTROL parameter. Specifying CONTROL=RoCE displays all the 10GbE RoCE Express TRLEs.	Shared Memory Communications over Remote Direct Memory Access
	V2R1	A new DEVSTATS operand is accepted. Specifying DEVSTATS=YES requests that VTAM obtain and display operational statistics for a 10GbE RoCE Express TRLE.	Shared Memory Communications over Remote Direct Memory Access
MODIFY CSDUMP	V2R1	The RNICTRLE operand is changed to accept the value MSGVALUE. Specifying RNICTRLE=MSGVALUE requests that VTAM take a diagnostic dump of the 10GbE RoCE Express interface identified in message IST2391I, IST2406I, or IST2419I. This diagnostic dump is taken in addition to any other requested diagnostic information.	Shared Memory Communications over RDMA adapter (RoCE) virtualization
	V2R1	A new RNICTLE operand is accepted. Specifying RNICTRLE requests that VTAM take a 10GbE RoCE Express diagnostic dump of the 10GbE RoCE Express interface represented by RNICTRLE in addition to any other diagnostic information requested.	Shared Memory Communications over Remote Direct Memory Access
MODIFY TOPO	V1R13	A new value, FUNCTION=CLRTREES, clears APPN routing trees. You should use this function only when advised by IBM service to do so.	Improved APPN routing resilience
MODIFY TRACE	V2R1	The maximum value of the BFRNUM operand when TYPE=ROUTE is specified is increased from 100 to 500 to allow up to 500 40K buffers for the APPN route selection trace.	SNA serviceability enhancements
MODIFY VTAMOPTS	V2R1	Changed to accept an IPv6 address or an IPv4 address for the IPADDR start option.	Enterprise Extender IPv6 address configuration

Command behavior changes

Table 33 on page 770 lists the SNA commands that have changed behavior.

For complete information about SNA commands, refer to the *z/OS Communications Server: SNA Operation*.

Table 33. Summary of new and changed Communications Server commands with changed behavior

Command	Release	Description of behavior change	Reason for change
DISPLAY BRFUSE	V2R1	Message group IST2403I is added to the command output. The message group provides details about VTAM's current usage of 64-bit storage, the maximum amount of 64-bit storage used, and any configured limit on the amount available to be used. The following messages are included in the message group to identify different types of 64-bit storage: • IST2404I describes VTAM's usage of HVCOMMON storage • IST2405I describes VTAM's usage of HVCOMMON storage for TRACE purposes • IST2412I describes VTAM's usage of FIXED HVCOMMON storage • IST2413I describes VTAM's usage of PRIVATE 64-bit storage • IST2414I describes VTAM's usage of FIXED PRIVATE 64-bit storage • IST2415I provides a total amount for all 64-bit storage usage	Shared Memory Communications over RDMA enhancements
DISPLAY EE	V2R1	IST2346I is added to output that contains information about a remote IP address or a remote host name.	Serviceability Enhancements
DISPLAY EEDIAG	V1R13	When TEST=YES and LIST=SUMMARY are specified together, messages IST2137I and IST2138I now have *NA for the hop count. Previously, IST2137I and IST2138I were displayed with the actual hop count.	Enterprise Extender firewall-friendly connectivity test
DISPLAY ID	V2R2	If the resource that is being displayed is an internal shared memory (ISM) TRLE, a new message group (IST2418I) is generated to display information unique to the ISM interface.	Shared Memory Communications - Direct Memory Access
	V2R1	If ID=*rnictrle_name* is specified and the 10GbE RoCE Express feature that *rnictrle_name* represents is operating in a shared RoCE environment, message IST2417I appears in the command output to display the associated virtual function number (VFN).	Shared Memory Communications over RDMA adapter (RoCE) virtualization
	V2R1	If the resource that is being displayed is a RNIC TRLE, a new message group (IST2361I) is generated to display information that is unique to the 10GbE RoCE Express interface.	Shared Memory Communications over Remote Direct Memory Access
	V2R1	When the ID represents a high performance routing (HPR) physical unit name, IST2395I is issued if the base mode adaptive rate-based (ARB) pacing algorithm is used.	Serviceability Enhancements

Table 33. Summary of new and changed Communications Server commands with changed behavior (continued)

Command	Release	Description of behavior change	Reason for change
DISPLAY ID	V1R13	When ID=*trlename* is specified for an active QDIO TRLE, messages IST2331I, IST2332 and one or more IST2333I are issued. For messages IST2331I, IST2332I, and IST2333I, a new QUEUE STATUS column now shows the current status of each read queue.	Performance improvements for Enterprise Extender traffic
	V1R13	The command is enhanced in the following ways: • Displays information about IQDX TRLEs • Includes the associated interface name on message IST1717I	HiperSockets optimization for intraensemble data networks
DISPLAY INOPDUMP	V2R2	If you enabled one or more of the new INOPDUMP control groups, you will get the following results: • Message IST1865I displays a new status of `ON BY CONTROL GROUP`. • Message IST1904I is be issued immediately after message IST1865I to display the current value of the INOPDUMP start option.	Shared Memory Communications - Direct Memory Access
DISPLAY STATS	V2R1	When you specify TYPE=CFS,STRNAME=EZBDVIPA, entries can also be displayed for IPv6 addresses.	Sysplex-Wide Security Associations for IPv6
	V1R13	When TYPE=VTAM is specified, existing message IST1227I displays the VIT size in megabytes. Message IST1227I for the status value 2 displays the VIT size. IST1227I for the status value 163 is retired.	Increased CTRACE and VIT capacity
DISPLAY TOPO	V1R13	When LIST=SUMMARY is specified and APPN routing trees were cleared, new message IST2360I displays the date and time of the last clear operation.	Improved APPN routing resilience
DISPLAY TRL	V2R2	If the TRLE operand specifies an ISM TRLE, a new message group (IST2418I) is generated to display information that is unique to the ISM interface.	Shared Memory Communications - Direct Memory Access
	V2R1	If TRLE=*rnictrle_name* is specified and the 10GbE RoCE Express feature that *rnictrle_name* represents is operating in a shared RoCE environment, message IST2417I appears in the command output to display the associated virtual function number (VFN).	Shared Memory Communications over RDMA adapter (RoCE) virtualization
	V2R1	When the TRLE operand specifies a RNIC TRLE, a new message group (IST2361I) is generated to display information that is unique to the 10GbE RoCE Express interface.	Shared Memory Communications over Remote Direct Memory Access
	V1R13	When TRLE=*trlename* is specified for an active QDIO TRLE, messages IST2331I, IST2332 and one or more IST2333I are issued. For messages IST2331I, IST2332I, and IST2333I a new QUEUE STATUS column now shows the current status of each read queue.	Performance improvements for Enterprise Extender traffic
	V1R13	The command is enhanced in the following ways: • Displays information about IQDX TRLEs • Includes the associated interface name on message IST1717I	HiperSockets optimization for intraensemble data networks

Table 33. Summary of new and changed Communications Server commands with changed behavior (continued)

Command	Release	Description of behavior change	Reason for change
DISPLAY VTAMOPTS	V2R1	When FORMAT=CURRENT is specified and the current IPADDR start option value is larger than 17 characters, message IST1904I is displayed instead of IST1189I.	Enterprise Extender IPv6 address configuration
	V2R1	When FORMAT=COMPLETE or FORMAT=MODIFIED is specified, and the IPADDR start option value is currently larger than 17 characters or was larger than 17 characters when VTAM was started, messages IST1905I, IST1906I, IST1907I, and IST1908I are displayed instead of IST1310I.	Enterprise Extender IPv6 address configuration
MODIFY NOTNSTAT MODIFY TNSTAT	V2R2	If you specify TRLE=*ISM_trle*, VTAM issues message IST1451I with *status* value set to FAILED. z/OS Communications Server supplies only tuning information for ISM devices as part of the Netstat DEvlinks/-d report or the GetIsms NMI.	Shared Memory Communications - Direct Memory Access
MODIFY TRACE	V1R13	A SIZE specification that is not specified in the valid range of 4M - 2048M inclusive is rejected. DSPSIZE is rejected.	Increased CTRACE and VIT capacity
MODIFY VTAMOPTS	V2R2	If you enabled one or more of the new INOPDUMP control groups on this command, you will get the following results: • Message IST1865I displays a new status of `ON BY CONTROL GROUP`. • Message IST1867I might display a new status of `SELECTIVELY PROCESSED`.	Shared Memory Communications - Direct Memory Access
	V2R1	When you specify the new PSRETRY IMMED operand value, activation of a TG or a change in the status of a TG triggers immediate path switch processing of HPR pipes.	HPR PSRETRY Enhancement

VTAM internal trace entries

In V1R13, the VTAM internal trace (VIT) table is relocated to 64-bit common (HCOMMON) storage. As a result, the IPCS subcommand VERBEXIT VTAMMAP functions are changed. VITAL does not support the ALL and ECSA operands and VTVIT does not set the DVIT, DVITC, DVITE, DVITL, and DVITO symbols. See Increased CTRACE and VIT capacity in *z/OS Communications Server: New Function Summary* for more information.

For complete information about VIT entries, see *z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT*.

Table 34 lists the new and changed VIT entries.

Table 34. Summary of new and changed Communications Server VTAM internal trace (VIT) entries

VIT entry	Release	Description	Related support
AFSM	V2R2	**Changed:** VIT record, SMC-D information added.	Shared Memory Communications - Direct Memory Access
	V2R1	**Changed:** VIT record, SMC-R information added.	Shared Memory Communications over Remote Direct Memory Access

Table 34. Summary of new and changed Communications Server VTAM internal trace (VIT) entries (continued)

VIT entry	Release	Description	Related support
ASN6	V2R2	**New:** VIT record, a continuation of the ASNB record.	64-bit enablement of the TCP/IP stack
CCR and CCR2	V2R1	**New:** VIT records to trace communication channel operations of 10GbE RoCE Express feature.	Shared Memory Communications over RDMA adapter (RoCE) virtualization
CHG6	V2R2	**New:** VIT record, a continuation of the CHGO record.	64-bit enablement of the TCP/IP stack
COPY and COP2	V1R13	**Deleted:** COPY and COP2 records are replaced with TOD record.	Increased CTRACE and VIT capacity
CPY6	V2R2	**New:** VIT record, a continuation of the CPYB record.	64-bit enablement of the TCP/IP stack
C64Q	V2R1	**New:** VIT record for IUTC64QM macro invocations.	Shared Memory Communications over Remote Direct Memory Access
C642	V2R1	**New:** VIT record, a continuation of the C64Q record.	Shared Memory Communications over Remote Direct Memory Access
DRBx	V2R1	**New:** VIT record for RoCE doorbell operations.	Shared Memory Communications over Remote Direct Memory Access
FIX6	V2R2	**New:** VIT record, a continuation of the FIXB record.	64-bit enablement of the TCP/IP stack
FRB6	V2R2	**New:** VIT record, a continuation of the FRBF record.	64-bit enablement of the TCP/IP stack
FR64	V2R2	**New:** VIT record for FRE64COMM or FRE64PVT requests.	Shared Memory Communications over RDMA enhancements
GTB6	V2R2	**New:** VIT record, a continuation of the GTBF record.	64-bit enablement of the TCP/IP stack
GT64	V2R2	**New:** VIT record for GET64COMM or GET64PVT requests.	Shared Memory Communications over RDMA enhancements
HCR	V2R1	**New:** VIT record for RoCE hardware command operations when the 10GbE RoCE Express feature operates in a dedicated RoCE environment.	Shared Memory Communications over Remote Direct Memory Access
HCR2	V2R1	**New:** VIT record, a continuation of the HCR record.	Shared Memory Communications over Remote Direct Memory Access
HCR3	V2R1	**New:** VIT record, a continuation of the HCR record.	Shared Memory Communications over Remote Direct Memory Access
HCR4	V2R1	**New:** VIT record, a continuation of the HCR record.	Shared Memory Communications over Remote Direct Memory Access
HCR5	V2R1	**New:** VIT record, a continuation of the HCR record.	Shared Memory Communications over Remote Direct Memory Access
ICR, ICR2, and ICR3	V2R2	**New:** VIT record for internal shared memory (ISM) control register operations.	Shared Memory Communications - Direct Memory Access
IOSP	V2R2	**Changed:** The VIT record can be displayed for internal shared memory (ISM) interfaces.	Shared Memory Communications - Direct Memory Access
	V2R1	**New:** VIT record for invocations of z/OS Peripheral Component Interconnect Express (PCIe) services.	Shared Memory Communications over Remote Direct Memory Access

Table 34. Summary of new and changed Communications Server VTAM internal trace (VIT) entries (continued)

VIT entry	Release	Description	Related support
IOS2	V2R2	**Changed:** The VIT record can be displayed for ISM interfaces.	Shared Memory Communications - Direct Memory Access
	V2R1	**New:** VIT record, a continuation of the IOSP record.	Shared Memory Communications over Remote Direct Memory Access
IOS3	V2R2	**Changed:** The VIT record can be displayed for ISM interfaces.	Shared Memory Communications - Direct Memory Access
	V2R1	**New:** VIT record, a continuation of the IOSP record.	Shared Memory Communications over Remote Direct Memory Access
IPLx and IPLA	V2R2	**New:** VIT record for an ISM polling operation.	Shared Memory Communications - Direct Memory Access
ISPx, ISP2, and ISP3	V2R2	**New:** VIT record for ISM operations.	Shared Memory Communications - Direct Memory Access
IUTR	V2R1	**New:** A variation of the IUTx VIT record, specifically for IUTIL-R invocations.	Shared Memory Communications over Remote Direct Memory Access
IUTX	V2R2	**Changed:** Added SMC-D information in existing VIT record.	Shared Memory Communications - Direct Memory Access
	V2R1	**Changed:** Added SMC-R information in existing VIT record.	Shared Memory Communications over Remote Direct Memory Access
IUT6	V2R2	**Changed:** Added SMC-D information in existing VIT record.	Shared Memory Communications - Direct Memory Access
	V2R2	**New:** VIT record, a continuation of the IUTx record.	64-bit enablement of the TCP/IP stack
ODTE	V2R1	**Changed:** Added SMC-R information in existing VIT record.	Shared Memory Communications over Remote Direct Memory Access
PAG6	V2R2	**New:** VIT record, a continuation of the PAGB record.	64-bit enablement of the TCP/IP stack
PCIx	V2R2	**Changed:** Added PCII variation that is defined for SMC-D processing	Shared Memory Communications - Direct Memory Access
PCIR	V2R2	**Changed:** Added SMC-D information in existing VIT record.	Shared Memory Communications - Direct Memory Access
	V2R2	**Changed:** Updated the Interrupt reason under offset 0x07 with new reason C'V'.	Release update
	V2R1	**New:** A variation of the PCIx record, specifically for interrupts of the 10GbE RoCE Express feature.	Shared Memory Communications over Remote Direct Memory Access
P64Q	V2R1	**New:** VIT record for IUTP64QM macro invocations.	Shared Memory Communications over Remote Direct Memory Access
P642	V2R1	**New:** VIT record, a continuation of the P64Q record.	Shared Memory Communications over Remote Direct Memory Access
QAP6	V2R2	**New:** VIT record, a continuation of the QAPL record.	64-bit enablement of the TCP/IP stack
QSRB	V2R2	**Changed:** Added SMC-D information in existing VIT record.	Shared Memory Communications - Direct Memory Access
	V2R1	**Changed:** Added SMC-R information in existing VIT record.	Shared Memory Communications over Remote Direct Memory Access
RAPB	V2R1	**New:** VIT record for RoCE anchor cell operations.	Shared Memory Communications over Remote Direct Memory Access

Table 34. Summary of new and changed Communications Server VTAM internal trace (VIT) entries (continued)

VIT entry	Release	Description	Related support
RAP2	V2R1	**New:** VIT record, a continuation of the RAPB record.	Shared Memory Communications over Remote Direct Memory Access
RCPI	V2R1	**New:** VIT record for RoCE input parameter list information.	Shared Memory Communications over Remote Direct Memory Access
RCPO	V2R1	**New:** VIT record for RoCE output parameter list information.	Shared Memory Communications over Remote Direct Memory Access
RCP2	V2R1	**New:** VIT record, a continuation of the RCPI and RCPO records.	Shared Memory Communications over Remote Direct Memory Access
RCP3	V2R1	**New:** VIT record, a continuation of the RCPO record.	Shared Memory Communications over Remote Direct Memory Access
RPLx	V2R1	**New:** VIT record for RoCE Poll operation completion.	Shared Memory Communications over Remote Direct Memory Access
RPLA	V2R1	**New:** VIT record, a continuation of the RPLx record.	Shared Memory Communications over Remote Direct Memory Access
RPLI	V2R1	**New:** VIT record, a continuation of the RPLA record.	Shared Memory Communications over Remote Direct Memory Access
RPLP	V2R1	**New:** VIT record, a continuation of the RPLx record.	Shared Memory Communications over Remote Direct Memory Access
RPSA	V2R2	**Changed:** Updated record bytes for SMC-D.	Shared Memory Communications - Direct Memory Access
	V2R1	**New:** VIT record, a continuation of the RPST record.	Shared Memory Communications over Remote Direct Memory Access
RPSI	V2R1	**New:** VIT record, a continuation of the RPSA record.	Shared Memory Communications over Remote Direct Memory Access
RPSP	V2R1	**New:** VIT record, a continuation of the RPST record.	Shared Memory Communications over Remote Direct Memory Access
RPST	V2R2	**Changed:** Updated record bytes for SMC-D.	Shared Memory Communications - Direct Memory Access
	V2R1	**New:** VIT record for RoCE Post operation completion.	Shared Memory Communications over Remote Direct Memory Access
RPS2	V2R1	**New:** VIT record, a continuation of the RPSA record.	Shared Memory Communications over Remote Direct Memory Access
RSLK	V2R1	**New:** VIT record for RoCE shared lock operations.	Shared Memory Communications over Remote Direct Memory Access
TOD	V2R1	**Changed:** Added CPU ID information.	Shared Memory Communications over Remote Direct Memory Access
	V1R13	**New:** Time of day snapshot.	Increased CTRACE and VIT capacity
VHCR, VHC2, VHC3, VHC4 and VHC5	V2R1	**New:** VIT records to trace VHCR commands of the 10GbE RoCE Express feature when the feature operates in a shared RoCE environment.	Shared Memory Communications over RDMA adapter (RoCE) virtualization
XB61	V2R2	**New:** VIT record for extended buffer list SPAC.	64-bit enablement of the TCP/IP stack
XB62	V2R2	**New:** VIT record, a continuation of the XB61 record.	64-bit enablement of the TCP/IP stack
XB63	V2R2	**New:** VIT record, a continuation of the XB61 record.	64-bit enablement of the TCP/IP stack

Communications Server summary of message changes for z/OS V2R2

The messages for Communications Server are documented in:

- *z/OS Communications Server: IP Messages Volume 1 (EZA)*
- *z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)*
- *z/OS Communications Server: IP Messages Volume 3 (EZY)*
- *z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)*
- *z/OS Communications Server: SNA Messages*

New

EZA5699I
EZA5700I
EZA5701I
EZA5702I
EZA5703I
EZA5704I
EZA5705I
EZA5706I
EZA5707I
EZA5708I
EZD1591I
EZD2029I
EZD2030I
EZD2031I
EZD2032I
EZD2033I
EZD2034I
EZD2040I
EZD2041I
EZZ0140I
EZZ0141I
EZZ0142I
EZZ0167I
EZZ0404I
EZZ2395I
EZZ2677I (1Q2016)
EZZ2678I (1Q2016)
EZZ2679I (1Q2016)
EZZ2680I (1Q2016)
EZZ2681I (1Q2016)
EZZ2683I (1Q2016)
EZZ3135I
EZZ6062I
EZZ6389I
IST2412I

IST2413I
IST2414I
IST2415I
IST2416I
IST2418I (1Q2016)
IST2419I
IST2420I (1Q2016)
IST2421I (1Q2016)
IST2422I (1Q2016)
IST2423I (1Q2016)
ISTM017I
ISTM018E
ISTM019I
ISTM020E
ISTM021I
ISTM022E
ISTM023I
ISTM024E
ISTM025I
ISTM026E
ISTM027I
ISTM028E
ISTM029I (1Q2016)
ISTM030E (1Q2016)
IVT5595I
IVT5596I
IVT5598I
IVT5603I
IVT5604I
IVT5605I
IVT5606I
IVT5607I

Changed

EZA8567I
EZA8593I
EZB2460E
EZBH008E
EZZ0307I
EZZ0312I
EZZ0323I
EZZ0327I
EZZ0356I
EZZ0358I
EZZ0378I (1Q2016)

EZZ0631I
EZZ0656I
EZZ4336I (1Q2016)
EZZ6035I (1Q2016)
EZZ6060I
EZZ6206I
EZZ6238I
EZZ7839I
EZZ7863I
EZZ7882I
EZZ8059I
EZZ8070I
EZZ8071I
EZZ8128I
EZZ8174I
EZZ8309I
EZZ8310I
EZZ8340I
EZZ8346I
EZZ8453I (1Q2016)
EZZ9298I
EZZ9304I
IST087I (1Q2016)
IST574E
IST1221I (1Q2016)
IST1314I (1Q2016)
IST1451I (1Q2016)
IST1717I (1Q2016)
IST1865I (1Q2016)
IST1904I (1Q2016)
IST2337I (1Q2016)
IST2361I
IST2390I (1Q2016)
IST2391I (1Q2016)
IST2392I (1Q2016)
IST2393I (1Q2016)
IST2403I
IST2405I
IST2407I (1Q2016)
IST2409I (1Q2016)
IST2411I (1Q2016)
IST2417I (1Q2016)
IST2419I (1Q2016)
ISTH001I
ISTH002I

ISTH017E
ISTM900I
IVT5501I
IVT5502I
IVT5507I
IVT5516I
IVT5517I
IVT5529I
IVT5538I
IVT5539I
IVT5549I
IVT5572I
IVT5573I
IVT5574I
IVT5594I

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Printed in USA