z/OS Communications Server

Documentation changes for APAR PH37372 Support for SMF compliance evidence

Version 2 Release 4

Version 2 Release 5

z/OS Communications Server

z/OS Communications Server

CONTENTS

NEW FUNCTION SUMMARY

Support for SMF compliance evidence

z/OS V2R4 and V2R5 Communications Server with APAR PH37372 generates new SMF type 1154 records that provide compliance evidence for the following components:

- TCP/IP stack – subtype 1
- FTP daemon – subtype 2
- TN3270E Telnet server – subtype 3
- CSSMTP client – subtype 4

This data can be helpful in determining compliance with various industry regulations and standards.

These records are generated whenever an Event Notification Facility (ENF) 86 signal is emitted by a system in the sysplex and the ENF 86 parameter list includes the local z/OS system name. The ENF 86 signal is triggered by a z/OSMF Compliance REST API.

Restrictions:

z/OS APARs OA61443 and OA61444 are required to support the new ENF 86 signal.

Dependencies:

- The TCP/IP stack must be active to provide the TCP/IP stack compliance evidence SMF record.
- The FTP daemon must be active to provide the FTP daemon compliance evidence SMF record.
- The TN3270E Telnet server must be active to provide TN3270E Telnet server compliance evidence SMF records (one per server port).
- CSSMTP must be active to provide the CSSMTP client compliance evidence record.

Using Support for SMF compliance evidence

To use Support for SMF compliance evidence, perform the tasks in *Table 1. Support for SMF compliance evidence*.

Table 1. Support for SMF compliance evidence

Task/Procedure	Reference
Review the data provided in the SMF 1154 records.	• SMF type 1154 records and Appendix F. Type 1154 SMF records in z/OS

	Communications Server: IP Programmer's Guide and Reference • Assembler mapping macro EZASM482 can be found in SYS1.MACLIB • C header mapping file can be found in SEZANMAC(EZA482) or /usr/include/eza482.h

Z/OS RELEASE UPGRADE REFERENCE SUMMARY

New and changed System Management Facilities (SMF) records for z/OS V2R5

This topic lists the System Management Facilities (SMF) records for z/OS elements and features that are new or changed for z/OS V2R5.

Table 3 provides a list of SMF records that are new or changed for z/OS V2R5. Detailed information about these SMF records can be found in one of the following documents, as indicated by the "Where documented" column in Table 3.

Communications Server:

- *Type 119 SMF records* in *z/OS Communications Server: IP Programmer's Guide and Reference*
- Type 1154 SMF records in z/OS Communications Server: IP Programmer's Guide and Reference
- *Tuning input/output (I/O) operations for RoCE connections* in *z/OS Communications Server: SNA Network Implementation Guide*

This topic lists the System Management Facilities (SMF) records for z/OS elements and features that are new or changed for z/OS V2R5.

Table 3. *New and changed System Management Facilities (SMF) records for z/OS V2R5*

SMF record	z/OS element or feature	Description	Where documented
Type 1154 • Subtype 1, TCP/IP stack compliance evidence record • Subtype 2, FTP daemon compliance evidence record • Subtype 3, TN3270E Telnet server compliance evidence record • Subtype 4, CSSMTP client	Communications Server	New SMF 1154 records **Reason for change:** Support for SMF compliance evidence (APAR PH37372)	Communications Server

compliance evidence record			

New and changed members in SYS1.MACLIB for z/OS V2R5

This topic lists the lists the new and changed members of SYS1.MACLIB for z/OS V2R5.

Table 4. *New and changed members in SYS1.MACLIB for z/OS V2R5*

Member	Element or feature	Description	Reason for change
EZASM482	Communications Server	New mapping for the SMF 1154, subtype 1 – 4 records	Support for SMF compliance evidence (APAR PH37372)

New and changed System Management Facilities (SMF) records for z/OS V2R4

This topic lists the System Management Facilities (SMF) records for z/OS elements and features that are new or changed for z/OS V2R4.

Table 5 provides a list of SMF records that are new or changed for z/OS V2R4. Detailed information about these SMF records can be found in one of the following documents, as indicated by the "Where documented" column in Table 5.

Communications Server:

- *Type 119 SMF records* in *z/OS Communications Server: IP Programmer's Guide and Reference*
- Type 1154 SMF records in z/OS Communications Server: IP Programmer's Guide and Reference
- *Tuning input/output (I/O) operations for RoCE connections* in *z/OS Communications Server: SNA Network Implementation Guide*

This topic lists the System Management Facilities (SMF) records for z/OS elements and features that are new or changed for z/OS V2R4.

Table 5. *New and changed System Management Facilities (SMF) records for z/OS V2R4*

SMF record	z/OS element or feature	Description	Where documented
Type 1154	Communications Server	New SMF 1154 records	Communications Server

• Subtype 1, TCP/IP stack compliance evidence record • Subtype 2, FTP daemon compliance evidence record • Subtype 3, TN3270E Telnet server compliance evidence record • Subtype 4, CSSMTP client compliance evidence record		**Reason for change:** Support for SMF compliance evidence (APAR PH37372)	

New and changed members in SYS1.MACLIB for z/OS V2R4

This topic lists the lists the new and changed members of SYS1.MACLIB for z/OS V2R4.

Table 6. *New and changed members in SYS1.MACLIB for z/OS V2R4*

Member	Element or feature	Description	Reason for change
EZASM482	Communications Server	New mapping for the SMF 1154, subtype 1 – 4 records	Support for SMF compliance evidence (APAR PH37372)

SMF records

Installations can use Systems Management Facilities (SMF) records for purposes such as performance management, capacity planning, auditing, and accounting. z/OS® Communications Server provides the following SMF record types:

- Type 109, Syslogd SMF records
- Type 118, event and interval records for TCP/IP and several applications; these records are no longer enhanced
- Type 119, event and interval records for TCP/IP and several applications; these records are continuing to be enhanced
- Type 1154, compliance evidence records for TCP/IP and several applications; these records are continuing to be enhanced

These records can be processed from the MVS™ SMF data sets or from SMF exits. Some of the records can also be processed programmatically by using the real-time SMF NMI. See Real-time TCP/IP network monitoring NMI for more information. See Type 109 SMF records, Type 118 SMF records, Type 119 SMF records and Type 1154 SMF records for detailed layouts of the records.

For general information about the uses of SMF records see z/OS Communications Server: IP Configuration Guide.

- SMF type 109 records
- SMF type 118 records
- SMF type 119 records
- SMF type 1154 records

SMF TYPE 1154 RECORDS

SMF type 1154 records provide compliance evidence for participating components with each component having a defined subtype. Communications Server provides SMF 1154 records for the TCP/IP stack, the FTP daemon, the TN3270E Telnet server, and the CSSMTP client.

SMF type 1154 records are generated when an ENF86 signal is received that requests compliance evidence for the local system. The ENF 86 signal is triggered by a z/OSMF Compliance REST API. For more information on REST API, see z/OS Compliance REST Interface in z/OSMF Programming Guide.

z/OS Communications Server

Communications Server provides compliance evidence in the following SMF 1154 subtypes:

- TCP/IP stack compliance evidence record (subtype 1)
- FTP daemon compliance evidence record (subtype 2)
- TN3270E Telnet server compliance evidence record (subtype 3)
- CSSMTP client compliance evidence record (subtype 4)

SMF type 1154 records utilize a common structure. Each record is organized as follows:

- SMF extended header
- SMF 1154 common self-defining section
- SMF 1154 common header
- SMF 1154, subtype-specific self-defining section
- Sections containing data for the record

You can parse the SMF type 1154 records that Communications Server generates by using macros and header files.

- For assembler applications, use the following macros which are installed in SYS1.MACLIB:
    - IFASMFH for the SMF extended header
    - IFAR1154 for the SMF 1154 common self-defining section and the common header
    - EZASM482 for the Communications Server subtype-specific mappings
- For C/C++ applications, use the following header files:
    - IFASMFH for the SMF extended header, which is installed in SYS1.SIEAHDR.H and /usr/include/zos
    - IFAR1154 for the SMF 1154 common self-defining section and the common header, which is installed in SYS1.SIEAHDR.H and /usr/include/zos
    - eza482.h for the Communications Server subtype specific mappings
        - This header file is installed in TCP/IP data set SEZANMAC, and in the /usr/include file system directory.

For the layout of SMF type 1154 records, see Appendix F. Type 1154 SMF records.

APPENDIX F. TYPE 1154 SMF RECORDS

SMF type 1154 records provide compliance evidence for participating components with each component having a defined subtype. Communications Server provides SMF 1154 records for the TCP/IP stack, the FTP daemon, the TN3270E Telnet server, and the CSSMTP client.

Each SMF 1154 record contains an SMF extended header, SMF 1154 common information, a subtype-specific self-defining section, and sections containing data for the record.

- **SMF extended header**

  SMF type 1154 records use the Extended SMF record header. For a definition of the extended header, see the *"Extended SMF record header Version 1" table* in Standard and extended SMF record headers in z/OS MVS System Management Facilities (SMF). The extended record type, SMFHDR1_EXT_RTY is set to 1154(x'482').

- **SMF 1154 common self-defining section and common header**

  For the common area mapping of Type 1154 SMF records common section, see Record common area mapping in z/OS MVS System Management Facilities (SMF).

Following the common header, each SMF 1154 has a subtype-specific section that describes its contents. Communications Server provides the following SMF 1154 SMF subtype records:

- TCP/IP stack compliance evidence record (subtype 1)
- FTP daemon compliance evidence record (subtype 2)
- TN3270E Telnet server compliance evidence record (subtype 3)
- CSSMTP client compliance evidence record (subtype 4)

Other SMF 1154 subtypes are provided by a number of z/OS components and applications. For a complete list of SMF 1154 subtypes, see Record type 1154 in z/OS MVS System Management Facilities (SMF).

This topic includes the following information:

Mapping SMF records

To allow an application to be able to process SMF 1154 records, z/OS Communications Server provides mapping macros and C header files.

- Assembler applications
  For assembler applications, use the following macros which are installed in SYS1.MACLIB:
  - IFASMFH for the SMF extended header
  - IFAR1154 for the SMF 1154 common self-defining section and the common header
  - EZASM482 for the Communications Server subtype-specific mappings

    EZASM482 produces assembler level DSECTs that can be used to map the various record formats described in this topic. When invoking EZASM482, all record mappings are created by default. Code NO for any of the operands to exclude those mappings from the assembler output.
- C/C++ applications

  For C/C++ applications, the following header files provide the SMF record mappings:
  - IFASMFH for the SMF extended header, which is installed in SYS1.SIEAHDR.H and /usr/include/zos
  - IFAR1154 for the SMF 1154 common self-defining section and the common header, which is installed in SYS1.SIEAHDR.H and /usr/include/zos
  - eza482.h for the Communications Server subtype specific mappings
    - This header file is installed in TCP/IP data set SEZANMAC, and in the /usr/include file system directory.

Standard data format concepts

The following concepts apply to standard data formats:

- IP addresses

  The IPv4 and IPv6 addresses are defined in the same 16-byte field in the record section. The IPv4 address is reported in the first 4 bytes of the field, and the IPv6 address occupies the whole field. A flag field in the record section indicates whether the field contains an IPv4 or an IPv6 address.
- Character data

  All character data is in EBCDIC using the IBM-1047 code page. The field values are left-justified and padded with trailing blanks to the maximum length of the field. If there is no value for the field it is set to blanks.

- Binary data

  All fields with a binary format are set to binary zeros if there is no value for the field.

SMF type 1154, subtype 1 –TCP/IP stack compliance evidence record

The TCP/IP stack compliance evidence record provides information on current TCP/IP profile settings for a specific TCP/IP stack.

If the SMF 1154 information exceeds 32,756 bytes, multiple records are created to provide the complete set of information. In the SMF 1154 common header SMF1154_C_RecordInd indicates whether "more records follow" and SMF1154_C_SeqNum indicates the sequence number. The sequence number starts at 0 in the first record and is incremented by 1 with each additional record.

The triplets in the 1154 subtype 1 specific section indicate which sections (and how many instances of the section) are included in the record.

Records within a set of records can be correlated using the extended record subtype (SMFHDR1_STP) from the extended SMF header and the system name (SMF1154_C_SystemName), sysplex name (SMF1154_C_SysplexName), jobname (SMF1154_C_Jobname), and request ID (SMF1154_C_RequestID) from the SMF 1154 common header.

Each record contains an SMF extended header, an SMF 1154 common triplets section, an SMF 1154 common header section, and an SMF 1154 subtype 1 specific section (self-defining section). The subtype specific section indicates the additional sections that are included in the record.

1154 subtype 1 specific section, self-defining section

This section defines the additional sections that are included in the record. A triplet is included for each defined section. The triplet includes the offset to the section from the start of the record, the length of a single instance of the section, and the number of instances of the section in the record.

Offset	Name	Length	Format	Description
0(x'00')	SMF1154_1_TRN	2	Binary	Number of triplets in this record (set to 9)
2(x'02')		2		Reserved (set to 0)
4(x'04')	SMF1154_1_S1_Offset	4	Binary	Offset to TCP/IP stack information

				section (from the start of the record)
8(x'08')	SMF1154_1_S1_Length	2	Binary	Length of TCP/IP stack information section
10(x'0A')	SMF1154_1_S1_Number	2	Binary	Number of TCP/IP stack information sections (set to 1)
12(x'0C')	SMF1154_1_S2_Offset	4	Binary	Offset to IPv4 configuration section (from the start of the record)
16(x'10')	SMF1154_1_S2_Length	2	Binary	Length of IPv4 configuration section
18(x'12')	SMF1154_1_S2_Number	2	Binary	Number of IPv4 configuration sections (set to 1)
20(x'14')	SMF1154_1_S3_Offset	4	Binary	Offset to IPv6 configuration section (from the start of the record)
24(x'18')	SMF1154_1_S3_Length	2	Binary	Length of IPv6 configuration section
26(x'1A')	SMF1154_1_S3_Number	2	Binary	Number of IPv6 configuration sections (set to 0 or 1)
28(x'1C')	SMF1154_1_S4_Offset	4	Binary	Offset to TCP configuration section (from the start of the record)

32(x'20')	SMF1154_1_S4_Length	2	Binary	Length of TCP configuration section
34(x'22')	SMF1154_1_S4_Number	2	Binary	Number of TCP configuration sections (set to 1)
36(x'24')	SMF1154_1_S5_Offset	4	Binary	Offset to UDP configuration section (from the start of the record)
40(x'28')	SMF1154_1_S5_Length	2	Binary	Length of UDP configuration section
42(x'2A')	SMF1154_1_S5_Number	2	Binary	Number of UDP configuration sections (set to 1)
44(x'2C')	SMF1154_1_S6_Offset	4	Binary	Offset to Global configuration section (from the start of the record)
48(x'30')	SMF1154_1_S6_Length	2	Binary	Length of Global configuration section
50(x'32')	SMF1154_1_S6_Number	2	Binary	Number of Global configuration sections (set to 1)
52(x'34')	SMF1154_1_S7_Offset	4	Binary	Offset to Port configuration section (from the start of the record)
56(x'38')	SMF1154_1_S7_Length	2	Binary	Length of Port configuration

				section
58(x'3A')	SMF1154_1_S7_Number	2	Binary	Number of Port configuration sections
60(x'3C')	SMF1154_1_S8_Offset	4	Binary	Offset to Management configuration section (from the start of the record)
64(x'40')	SMF1154_1_S8_Length	2	Binary	Length of Management configuration section
66(x'42')	SMF1154_1_S8_Number	2	Binary	Number of Management configuration sections (set to 1)
68(x'44')	SMF1154_1_S9_Offset	4	Binary	Offset to Network access configuration section (from the start of the record)
72(x'48')	SMF1154_1_S9_Length	2	Binary	Length of Network access configuration section
74(x'4A')	SMF1154_1_S9_Number	2	Binary	Number of Network access configuration sections

TCP/IP stack information section

Offset	Name	Length	Format	Description

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_PICOEye	4	EBCDIC	Identifier - 'PICO'
4(X'4')	SMF1154_1_PICOStartTime	8	Binary	**Time TCP/IP stack was started** (TOD clock value)
12(X'C')	SMF1154_1_PICOStartDate	4	Packed	**Date TCP/IP stack was started**
16(X'10')	SMF1154_1_PICOSysplexGrpName	8	EBCDIC	**Sysplex group name**. The value is populated when the TCP/IP stack joins the sysplex group. If the TCP/IP stack has never joined the sysplex group since it was initialized, this field is set to blanks.
24(x'18')	SMF1154_1_PICOIpv6	1	Binary	**IPv6 support** 0 - IPv6 is not enabled on this TCP/IP stack 1 - IPv6 is enabled on this TCP/IP stack Configured in the BPXPRMxx parmlib member for this TCP/IP stack.
25(x'19')		3		Reserved. Set to 0.

IPv4 configuration section

The information that is provided in the IPv4 configuration section reflects fields that are configured on the IPCONFIG statement in the TCP/IP profile unless otherwise noted.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_V4CFEye	4	EBCDIC	Identifier – 'V4CF'
4(X'4')	SMF1154_1_V4CFDatagramFwd	1	Binary	**IPv4 Datagram forwarding** 0 - Stack is not forwarding IPv4 datagrams 1 - Stack is forwarding IPv4 datagrams Configured with the DATAGRAMFWD / NODATAGRAMFWD parameter.
5(X'5')	SMF1154_1_V4CFDynamicXcf	1	Binary	**IPv4 Dynamic XCF interfaces defined** 0 - IPv4 dynamic XCF interfaces are not defined 1 - IPv4 dynamic XCF interfaces are

Offset	Name	Length	Format	Description
				defined and the following fields contain dynamic XCF configured values: • SMF1154_1_V4CFDynXcfAddr • SMF1154_1_V4CFDynXcfMask • SMF1154_1_V4CFDynXcfSecClass Configured with the DYNAMICXCF / NODYNAMICXCF parameter.
6(X'6')	SMF1154_1_V4CFIgnRedirectCfg	1	Binary	**Ignore ICMP redirects configured** 0 - Ignore ICMP redirects is not configured in the TCP/IP profile 1 - Ignore ICMP redirects is configured in the TCP/IP profile Configured with the IGNOREREDIRECT parameter.
7(X'7')	SMF1154_1_V4CFIgnRedirectAct	1	Binary	**Ignore ICMP redirects active** 0 - ICMP redirects are not ignored 1 - ICMP redirects are ignored, SMF1154_1_V4CFIgnRedirectRsn indicates the reason why ICMP redirects are being ignored.
8(X'8')	SMF1154_1_V4CFIPSecurity	1	Binary	**IP security enabled for IPv4** 0 - IP security is not enabled for IPv4 1 - IP security is enabled for IPv4 Configured with the IPSECURITY parameter.
9(X'9')	SMF1154_1_V4CFDVIPSec	1	Binary	**IPsec tunnels eligible for sysplex-wide distribution and takeover** 0 = Sysplex-wide tunnels are not enabled. 1 = Sysplex-wide tunnels are enabled for both IPv4 and IPv6. Configured with the DVIPSEC parameter on the IPSEC statement in the TCP/IP profile.

Offset	Name	Length	Format	Description
10(X'A')		2		Reserved. Set to 0.
12(X'C')	SMF1154_1_V4CFArpTimeout	4	Binary	**ARP cache timeout for LCS devices** ARP cache timeout in seconds for LAN channel station (LCS) devices. The value is in the range of 60 – 86400 seconds. This value can be configured on the ARPAGE statement or on the ARPTO parameter of the IPCONFIG statement in the TCP/IP profile.
16(X'10')	SMF1154_1_V4CFDynXcfAddr	4	Binary	**Dynamic XCF IPv4 address** This field is valid if SMF1154_1_V4CFDynamicXcf is set to 1. Configured with the DYNAMICXCF parameter.
20(X'14')	SMF1154_1_V4CFDynXcfMask	1	Binary	**Dynamic XCF number of mask bits** This field is valid if SMF1154_1_V4CFDynamicXcf is set to 1. This field has a value from 1 – 32. Configured with the DYNAMICXCF parameter.
21(X'15')	SMF1154_1_V4CFDynXcfSecClass	1	Binary	**Dynamic XCF security class** This field is valid if SMF1154_1_V4CFDynamicXcf is set to 1. Security class value (1 – 255) assigned to the XCF interface for use with IP filtering. Configured with the DYNAMICXCF SECCLASS parameter.
22(X'16')	SMF1154_1_V4CFIgnRedirectRsn	1	Binary	**Reason ICMP Redirects ignored** This field is valid if

Offset	Name	Length	Format	Description
				SMF1154_1_V4CFIgnRedirectAct is set to 1. SMF1154_1_V4CFIgnRedRsn_CFG (1) – IGNOREREDIRECT parameter configured on the IPCONFIG statement in the TCP/IP profile SMF1154_1_V4CFIgnRedRsn_OMP (2) – OMPROUTE set ignore redirects SMF1154_1_V4CFIgnRedRsn_IDS (3) – IDS policy configured to discard ICMP Redirects
23(X'17')	SMF1154_1_V4CFReasmTimeout	1	Binary	**Reassembly timeout** Reassembly timeout value in seconds. The value is in the range of 1 – 240 seconds. Configured with the REASSEMBLYTIMEOUT parameter.
24(X'18')	SMF1154_1_V4CFTTL	1	Binary	**Time to Live** Time to live or hop limit for an IPv4 packet. The value is in the range of 1 – 255. Configured with the TTL parameter.
25(x'19')		3	Binary	Reserved. Set to 0.

IPv6 configuration section

The information that is provided in the IPv6 configuration section reflects fields that are configured on the IPCONFIG6 statement in the TCP/IP profile unless otherwise noted. This section is included if IPv6 is enabled for the TCP/IP stack (SMF1154_1_PICOIpv6 = 1).

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_V6CFEye	4	EBCDIC	Identifier – 'V6CF'
4(X'4')	SMF1154_1_V6CFDatagram	1	Binary	**IPv6 datagram forwarding**

Offset	Name	Length	Format	Description
	Fwd			0 - Stack is not forwarding IPv6 datagrams 1 - Stack is forwarding IPv6 datagrams Configured with the DATAGRAMFWD / NODATAGRAMFWD parameter.
5(X'5')	SMF1154_1_V6CFDynamicXcf	1	Binary	**IPv6 Dynamic XCF interfaces defined** 0 - IPv6 dynamic XCF interfaces are not defined 1 - IPv6 dynamic XCF interfaces are defined and the following fields contain dynamic XCF configured values: • SMF1154_1_V6CFDynXcfAddr • SMF1154_1_V6CFDynXcfPfxRteLen • SMF1154_1_V6CFDynXcfSecClass Configured with the DYNAMICXCF / NODYNAMICXCF parameter.
6(X'6')	SMF1154_1_V6CFDynXcfIfIDFlg	1	Binary	**Dynamic XCF IPv6 Interface ID configured** This field is valid if SMF1154_1_V6CFDynamicXcf is set to 1. 0 - No IPv6 interface ID configured. Link-local address generated with a random value. 1 - IPv6 interface ID configured and contained in the SMF1154_1_V6CFDynXcfIntrID field. Link-local address generated with the specified value. Configured with the DYNAMICXCF INTFID parameter.
7(X'7')	SMF1154_1_V6CFIgnRedirectCfg	1	Binary	**Ignore ICMPv6 redirects configured** 0 - Ignore ICMPv6 redirects is not configured in the TCP/IP profile 1 - Ignore ICMPv6 redirects is configured

Offset	Name	Length	Format	Description
				in the TCP/IP profile Configured with the IGNOREREDIRECT parameter.
8(X'8')	SMF1154_1_V6CFIgnRedirectAct	1	Binary	**Ignore ICMPv6 redirects active** 0 - ICMPv6 redirects are not ignored 1 - ICMPv6 redirects are ignored, SMF1154_1_V6CFIgnRedirectRsn indicates the reason why ICMPv6 redirects are being ignored.
9(X'9')	SMF1154_1_V6CFIgnoreRtrHopLim	1	Binary	**Ignore router advertised hop limit** 0 – Do not ignore router advertised hop limits. 1 – Ignore router advertised hop limits. Configured with the IGNOREROUTERHOPLIMIT / NOIGNOREROUTERHOPLIMIT parameter.
10(X'A')	SMF1154_1_V6CFIPSecurity	1	Binary	**IP security enabled for IPv6** 0 - IP security is not enabled for IPv6 1 - IP security is enabled for IPv6 Configured with the IPSECURITY parameter.
11(X'B')		1		Reserved. Set to 0
12(X'C')	SMF1154_1_V6CFDynXcfIntfID	8	Binary	**Dynamic XCF IPv6 interface ID** This field is valid if SMF1154_1_V6CFDynXcfIfIDFlg is set to 1. Configured with the DYNAMICXCF INTFID parameter.
20(X'14')	SMF1154_1_V6CFDynXcfAddr	16	Binary	**Dynamic XCF IPv6 address** This field is valid if SMF1154_1_V6CFDynamicXcf is set to 1. Configured with the DYNAMICXCF

Offset	Name	Length	Format	Description
				parameter.
36(X'24')	SMF1154_1_V6CFDynXcfPfxRteLen	1	Binary	**Dynamic XCF prefix route length** This field is valid if SMF1154_1_V6CFDynamicXcf is set to 1. The field is a value from 1 – 128. Configured with the DYNAMICXCF parameter.
37(X'25')	SMF1154_1_V6CFDynXcfSecClass	1	Binary	**Dynamic XCF security class** This field is valid if SMF1154_1_V6CFDynamicXcf is set to 1. Security class value (1 – 255) assigned to the IPv6 XCF interface for use with IP filtering. Configured with the DYNAMICXCF SECCLASS parameter.
38(X'26')	SMF1154_1_V6CFHopLimit	1	Binary	**IPv6 hop limit** Hop limit for an IPv6 packet. The value is in the range of 1 – 255. Configured with the HOPLIMIT parameter.
39(X'27')	SMF1154_1_V6CFIcmpErrLimit	1	Binary	**ICMPv6 error rate limit** Number of ICMPv6 error messages (1 – 20) that can be sent to a particular IPv6 destination per second. Configured with the ICMPERRORLIMIT parameter.
40(X'28')	SMF1154_1_V6CFIgnRedirectRsn	1	Binary	**Reason ICMPv6 Redirects ignored** This field is valid if SMF1154_1_V6CFIgnRedirectAct is set to 1. SMF1154_1_V6CFIgnRedRsn_CFG (1) – IGNOREREDIRECT parameter configured on the IPCONFIG6 statement in the

Offset	Name	Length	Format	Description
				TCP/IP profile SMF1154_1_V6CFIgnRedRsn_OMP (2) – OMPROUTE set ignore redirects SMF1154_1_V6CFIgnRedRsn_IDS (3) – IDS policy configured to discard ICMP6 Redirects
41(X'29')	SMF1154_1_V6CFOSMSecClass	1	Binary	**OSM security class** Security class value (1 – 255) assigned to each OSM interface for use with IP filtering. Configured with the OSMSECCLASS parameter.
42(X'2A')		2		Reserved. Set to 0.

TCP configuration section

The information that is provided in the TCP configuration section reflects fields that are configured on the TCPCONFIG statement in the TCP/IP profile unless otherwise noted.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_TCCFEye	4	EBCDIC	Identifier – 'TCCF'
4(X'4')	SMF1154_1_TCCFRestrictLowPorts	1	Binary	**Restrict TCP low ports** 0 – TCP ports 1-1023 are not restricted 1 – TCP ports 1-1023 are restricted Configured with the RESTRICTLOWPORTS / UNRESTRICTLOWPORTS parameter
5(X'5')	SMF1154_1_TCCFTimeStamp	1	Binary	**TCP timestamp option enabled** 0 – TCP timestamp option is not enabled 1 – TCP timestamp option is enabled Configured with the TCPTIMESTAMP /

Offset	Name	Length	Format	Description
				NOTCPTIMESTAMP parameter
6(X'6')	SMF1154_1_TCCFTtls	1	Binary	**AT-TLS function activated** 0 - Application transparent Transport Layer Security (AT-TLS) is not active for the TCP/IP stack. 1 – AT-TLS is active for the TCP/IP stack. Configured with the TTLS / NOTTLS parameter
7(X'7')		1		Reserved. Set to 0.
8(X'8')	SMF1154_1_TCCFEphemPortBegNum	2	Binary	**TCP ephemeral port range start** The starting port for the range of ephemeral ports to be assigned when the bind is done. The value can be in the range 1024 – 65535. Configured with the EPHEMERALPORTS parameter.
10(X'A')	SMF1154_1_TCCFEphemPortEndNum	2	Binary	**TCP ephemeral port range end** The ending port for the range of ephemeral ports to be assigned when the bind is done. The value can be in the range 1024 – 65535. Configured with the EPHEMERALPORTS parameter.
12(X'C')	SMF1154_1_TCCFSoMaxConn	4	Binary	**Maximum queued connection requests** The maximum number of pending connection requests queued for any TCP listening socket. The value is in the range of 1-2147483647. Configured with the SOMAXCONN statement in the TCP/IP profile.
16(X'10')	SMF1154_1_TCCFFinWait2Time	2	Binary	**FINWAIT2 interval** The number of seconds a TCP connection should remain in the FINWAIT2 state. The value is in the range 1 – 3600 seconds.

Offset	Name	Length	Format	Description
				Configured with the FINWAIT2TIME parameter.
18(X'12')	SMF1154_1_TCCFTimeWaitInterval	2	Binary	**TIMEWAIT interval** The number of seconds a TCP connection remains in the TIMEWAIT state. The value is in the range 0 – 120 seconds. Configured with the TIMEWAITINTERVAL parameter.

UDP configuration section

The information that is provided in the UDP configuration section reflects fields that are configured on the UDPCONFIG statement in the TCP/IP profile unless otherwise noted.

Offset	Name	Length	Format	Description
0(X'00')	SMF1154_1_UDCFEye	4	EBCDIC	Identifier – 'UDCF'
4(X'4')	SMF1154_1_UDCFRestrictLowPorts	1	Binary	**Restrict UDP low ports** 0 – UDP ports 1-1023 are not restricted 1 – UDP ports 1-1023 are restricted Configured with the RESTRICTLOWPORTS / UNRESTRICTLOWPORTS parameter
5(X'5')	SMF1154_1_UDCFChkSum	1	Binary	**UDP checksum required** 0 – UDP layer does not perform checksum processing for IPv4 packets 1 – UDP layer performs checksum processing for IPv4 packets. Configured with the UDPCHKSUM / NOUDPCHKSUM parameter
6(X'6')	SMF1154_1_UDCFQueueLimit	1	Binary	**UDP queue limit enabled** 0 – No queue limit set for UDP. 1 – Queue limit set for UDP. Maximum of 2000 incoming datagrams are queued on a UDP socket.

				Configured with the UDPQUEUELIMIT / NOUDPQUEUELIMIT parameter
7(X'7')		1		Reserved. Set to 0.
8(X'8')	SMF1154_1_UDCFEphemPortBegNum	2	Binary	**UDP ephemeral port range start** The starting port for the range of ephemeral ports to be assigned when the bind is done. The value can be in the range 1024 - 65535. Configured with the EPHEMERALPORTS parameter.
10(X'A')	SMF1154_1_UDCFEphemPortEndNum	2	Binary	**UDP ephemeral port range end** The ending port for the range of ephemeral ports to be assigned when the bind is done. The value can be in the range 1024 - 65535. Configured with the EPHEMERALPORTS parameter.

Global configuration section

The information that is provided in the global configuration section reflects fields that are configured on the GLOBALCONFIG statement in the TCP/IP profile unless otherwise noted.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_GBCFEye	4	EBCDIC	Identifier – 'GBCF'
4(X'4')	SMF1154_1_GBCFExpBindPortRange	1	Binary	**Explicit bind port range defined** 0 – TCP/IP stack does not participate in the allocation of ports from a pool guaranteed to be unique across the sysplex. 1 – TCP/IP stack participates in the allocation of ports from a pool 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. The following fields contain the port range values: • SMF1154_1_GBCFExpBindPortBe

Offset	Name	Length	Format	Description
				• gNm • SMF1154_1_GBCFExpBindPortEndNm Configured with the EXPLICITBINDPORTRANGE / NOEXPLICITBINDPORTRANGE parameter.
5(X'5')	SMF1154_1_GBCFMlsChkTerminate	1	Binary	**MLS check terminate** 0 – TCP/IP stack is not terminated when inconsistent configuration information is discovered in a multilevel-secure environment. 1 – TCP/IP stack is terminated when inconsistent configuration information is discovered in a multilevel-secure environment. Configured with MLSCHKTERMINATE / NOMLSCHKTERMINATE parameter.
6(X'6')	SMF1154_1_GBCFSMCR	1	Binary	**SMC-R enabled** 0 – TCP/IP stack should not use Shared Memory Communications over Remote Direct Memory Access (SMC-R) 1 – TCP/IP stack should use SMC-R Configured with the SMCR / NOSMCR parameter
7(X'7')	SMF1154_1_GBCFSMCD	1	Binary	**SMC-D enabled** 0 – TCP/IP stack should not use Shared Memory Communications – Direct Memory Access (SMC-D) 1 – TCP/IP stack should use SMC-D Configured with the SMCD / NOSMCD parameter
8(X'8')	SMF1154_1_GBCFAutoSMC	1	Binary	**SMC auto-monitoring** 0 – TCP/IP stack does not monitor inbound TCP connections to determine whether the connections can benefit from

Offset	Name	Length	Format	Description
				using SMC. 1 – TCP/IP stack monitors inbound TCP connections to determine whether the connections can benefit from using SMC. Configured with the AUTOSMC / NOAUTOSMC parameter
9(X'9')	SMF1154_1_GBCFZERT	1	Binary	**zERT enabled** 0 – TCP and Enterprise Extender traffic will not be monitored by z/OS Encryption Readiness Technology (zERT) 1 – TCP and Enterprise Extender traffic will be monitored by zERT Configured with the ZERT / NOZERT parameter.
10(X'A')	SMF1154_1_GBCFZERTAGG	1	Binary	**zERT aggregation enabled** 0 – zERT aggregation is not enabled 1 – zERT aggregation is enabled Configured with the ZERT AGGREGATION / ZERT NOAGGREGATION
11(X'B')	SMF1154_1_GBCFSysMonNoJoin	1	Binary	**Sysplex monitor – no join** 0 – TCP/IP stack joins the TCP/IP sysplex group (EZBTCPCS) during stack initialization based on DELAYJOIN and DELAYJOINIPSEC settings. 1 – TCP/IP stack does not join the TCP/IP sysplex group (EZBTCPCS) during stack initialization. Configured with the SYSPLEXMONITOR NOJOIN parameter
12(X'C')	SMF1154_1_GBCFSysMonDelayJoin	1	Binary	**Sysplex monitor – OMPROUTE delay join** 0 – TCP/IP stack does not delay joining the sysplex group waiting for OMPROUTE to be active. 1 – TCP/IP stack delays joining or rejoining the sysplex group until

Offset	Name	Length	Format	Description
				OMPROUTE is active. Configured with the SYSPLEXMONITOR DELAYJOIN/ SYSPLEXMONITOR NODELAYJOIN parameter
13(X'D')	SMF1154_1_GBCFSysMonDelayJoinI	1	Binary	**Sysplex monitor – IPsec delay join** 0 – TCP/IP stack does not delay joining the sysplex group waiting for the IPsec infrastructure to be active and operational. 1 – TCP/IP stack delays joining or rejoining the sysplex group until the IPsec infrastructure is active and operational. Configured with the SYSPLEXMONITOR DELAYJOINIPSEC/ SYSPLEXMONITOR NODELAYJOINIPSEC parameter
14(X'E')	SMF1154_1_GBCFSysMonIpsec	1	Binary	**Sysplex monitor – monitor IPsec** 0 - TCP/IP stack does not monitor the IPsec infrastructure after the stack has joined the sysplex group. 1 – TCP/IP stack monitors the IPsec infrastructure after the stack has joined the sysplex group, to detect if it becomes inactive or non-operational. Configured with the SYSPLEXMONITOR DELAYJOINIPSEC MONIPSEC / SYSPLEXMONITOR DELAYJOINIPSEC NOMONIPSEC parameter
15(X'F')	SMF1154_1_GBCFSysMonMonIntf	1	Binary	**Sysplex monitor – monitor interfaces** 0 – TCP/IP stack does not monitor the status of specified network interfaces. 1 – TCP/IP stack monitors the status of specified network interfaces. Configured with SYSPLEXMONITOR MONITORINTERFACE / SYSPLEXMONITOR NOMONITORINTERFACE parameter

Offset	Name	Length	Format	Description
16(X'10')	SMF1154_1_GBCFSysMonDynRoute	1	Binary	**Sysplex monitor - dynamic routes** 0 – TCP/IP stack does not monitor the presence of dynamic routes over monitored interfaces. 1 – TCP/IP stack monitors the presence of dynamic routes over monitored interfaces. Configured with the SYSPLEXMONITOR MONITORINTERFACE DYNROUTE / NODYNROUTE parameter
17(X'11')	SMF1154_1_GBCFSysMonRecovery	1	Binary	**Sysplex monitor – recovery** 0 – TCP/IP stack does not leave the sysplex group when a problem is detected. 1 – TCP/IP stack leaves the sysplex group when a problem is detected. Configured with the SYSPLEXMONITOR RECOVERY / SYSPLEXMONITOR NORECOVERY parameter
18(X'12')	SMF1154_1_GBCFSysMonAutoRejoin	1	Binary	**Sysplex monitor - auto-rejoin** 0 – TCP/IP stack does not automatically rejoin the sysplex group after detected problems are resolved 1 – TCP/IP stack automatically rejoins the sysplex group after detected problems are resolved Configured with the SYSPLEXMONITOR AUTOREJOIN / SYSPLEXMONITOR NOAUTOREJOIN parameter
19(X'13')		1	Binary	Reserved. Set to 0.
20(X'14')	SMF1154_1_GBCFSysMonTimerSecs	2	Binary	**Sysplex monitor timer** The number of seconds used by the sysplex monitor function to react to problems with needed sysplex resources. Valid values are in the range 10-3600 seconds.

Offset	Name	Length	Format	Description
				Configured with the SYSPLEXMONITOR TIMERSECS parameter
22(X'16')	SMF1154_1_GBCFIqdVlanId	2	Binary	**VLAN ID for dynamic XCF hipersockets interface** The VLAN ID used when Hipersockets (iQDIO) connectivity is used for dynamic XCF support. If not configured, the value is 0. Configured with the IQDVLANID parameter
24(X'18')	SMF1154_1_GBCFXcfGroupID	2	EBCDIC	**TCP XCF group ID suffix** The 2-digit suffix used to generate the sysplex group name that the TCP/IP stack joins. Valid values are in the range 2-31. If not configured, the field is set to blanks. Configured with the XCFGRPID parameter
26(X'1A')	SMF1154_1_GBCFExpBindPortBegNm	2	Binary	**Explicit bind port range start** This field is valid if SMF1154_1_GBCFExpBindPortRange is set to 1. The starting port for the range of ports to be assigned when an explicit bind of a TCP socket is done to the IPv4 INADDR_ANY or IPv6 unspecified address (in6addr_any), and port 0. The value can be in the range 1024 - 65535. Configured with EXPLICITBINDPORTRANGE parameter.
28(X'1C')	SMF1154_1_GBCFExpBindPortEndNm	2	Binary	**Explicit bind port range end** This field is valid if SMF1154_1_GBCFExpBindPortRange is set to 1. The ending port for the range of ports to be assigned when an explicit bind of a TCP socket is done to the IPv4 INADDR_ANY

Offset	Name	Length	Format	Description
				or IPv6 unspecified address (in6addr_any), and port 0. The value can be in the range 1024 - 65535. Configured with the EXPLICITBINDPORTRANGE parameter
30(X'1E')	SMF1154_1_GBCFAutoIQDC	1	Binary	**Dynamic IQD converged interfaces** 0 - Dynamic IQD (HiperSockets) converged interfaces are not used. 1 – Dynamic IQD (HiperSockets) converged interfaces are used for eligible traffic. Configured with the AUTOIQDC / NOAUTOIQDC parameter
31(X'1F')		1	Binary	Reserved. Set to 0

Port configuration section

The information that is provided in a port configuration section entry reflects fields that are configured on the PORT or PORTRANGE statement in the TCP/IP profile unless otherwise noted. There can be multiple instances of this section in the record, one per PORT or PORTRANGE sub statement.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_PORTEye	4	EBCDIC	Identifier – 'PORT'
4(X'4')	SMF1154_1_PORTRange	1	Binary	**PORTRANGE entry** 0 – Entry is for a single port (PORT statement) 1 – Entry is for a range of ports (PORTRANGE statement) Configured with the PORT or PORTRANGE statement
5(X'5')	SMF1154_1_PORTUnrsv	1	Binary	**Unreserved port entry** 0 – Entry applies to a reserved port or ports 1 – Entry applies to an unreserved port Configured with the UNRSV parameter on

Offset	Name	Length	Format	Description
				the PORT statement
6(X'6')	SMF1154_1_PORTTCP	1	Binary	**TCP port entry** 0 – UDP port entry 1 – TCP port entry Configured with the TCP and UDP parameters on the PORT or PORTRANGE statements
7(X'7')	SMF1154_1_PORTUseType	1	Binary	**Port use type** Type of use for the port or ports. SMF1154_1_PORTUTReserved(1) None of the ports can be used by any user for the protocol (TCP or UDP) specified on this entry. This type applies only to reserved port entries (SMF1154_1_PORTUnrsv=0) SMF1154_1_PORTUTAuthport(2) The ports can be used only by the FTP server when the server is configured to use PASSIVEDATAPORTS. This type applies only to reserved port entries (SMF1154_1_PORTUnrsv=0) which were reserved as a range (SMF1154_1_PORTRange is set to 1). SMF1154_1_PORTUTJobname(3) The specified or unreserved port(s) can be used only based on an MVS job name value. If this use type value is set, then field SMF1154_1_PORTJobName contains the job name value. Configured with the RESERVED, jobname, or AUTHPORT parameter on the PORT or PORTRANGE statement. AUTHPORT can only be configured on PORTRANGE.
8(X'8')	SMF1154_1_PORTRSaf	1	Binary	**Reserved port SAF configured**

Offset	Name	Length	Format	Description
				This field is valid for a reserved (SMF1154_1_PORTUnrsv = 0) jobname entry (SMF1154_1_PORTUseType = SMF1154_1_PORTUTJobname). 0 – SAF resource name is not configured for the entry. 1 – A SAF resource name is configured for the entry and SMF1154_1_PORTSafName contains the name. Configured with the SAF parameter on the PORT or PORTRANGE statement.
9(X'9')	SMF1154_1_PORTRNoSMC	1	Binary	**Reserved port NOSMC** 1 – Override the setting of SMCGLOBAL AUTOSMC and do not allow SMC for inbound TCP connections that use this port If both SMF1154_1_PORTRNoSMC and SMF1154_1_PORTRSMC are 0, use the SMCGLOBAL AUTOSMC setting. Configured with the NOSMC parameter on the PORT or PORTRANGE statement
10(X'A')	SMF1154_1_PORTRSMC	1	Binary	**Reserved port SMC** 1 – Override the setting of SMCGLOBAL AUTOSMC and attempt to use SMC for inbound TCP connections that use this port. If both SMF1154_1_PORTRNoSMC and SMF1154_1_PORTRSMC are 0, use the SMCGLOBAL AUTOSMC setting. Configured with the SMC parameter on the PORT or PORTRANGE statement
11(X'B')		1	Binary	Reserved. Set to 0.
12(X'C')	SMF1154_1_PORTBegNum	2	Binary	**Reserved port range start**

Offset	Name	Length	Format	Description
				This field is valid for a reserved port entry (SMF1154_1_PORTUnrsv = 0) and contains one of the following values: • The reserved port number, if SMF1154_1_PORTRange = 0. • The beginning reserved port number in the range, if SMF1154_1_PORTRange = 1. Configured on the PORT or PORTRANGE statement.
14(X'E')	SMF1154_1_PORTEndNum	2	Binary	**Reserved port range end** This field is valid for a reserved port range entry (SMF1154_1_PORTUnrsv = 0 and SMF1154_1_PORTRange = 1). It is the ending reserved port number in the range. Based on the configuration of the port and number of ports on the PORTRANGE statement
16(X'10')	SMF1154_1_PORTUDeny	1	Binary	**Unreserved port deny** This field is valid for an unreserved entry (SMF1154_1_PORTUnrsv = 1). 0 – Deny access to all unreserved ports is not configured. 1 – Access to all unreserved ports is denied for the protocol (TCP or UDP) configured in this entry. Configured with the DENY parameter on the PORT statement.
17(X'11')	SMF1154_1_PORTUSaf	1	Binary	**Unreserved port SAF configured** This field is valid for an unreserved entry (SMF1154_1_PORTUnrsv = 1). 0 – SAF resource name is not configured for the entry 1 – A SAF resource name is configured for

Offset	Name	Length	Format	Description
				the entry and SMF1154_1_PORTSafName contains the name. Binding to, or listening on, any unreserved port is restricted to users that are permitted to the specified SAF SERVAUTH resource. Configured with the SAF parameter on the PORT statement.
18(X'12')		2	Binary	Reserved. Set to 0.
20(X'14')	SMF1154_1_PORTJobName	8	EBCDIC	**Job name** This field is valid if SMF1154_1_PORTUseType is SMF1154_1_PORTUTJobname. This field contains the MVS job name value associated with the port entry, padded with trailing blanks. Configured on the PORT or PORTRANGE statement
28(X'1C')	SMF1154_1_PORTSafName	8	EBCDIC	**SAF resource name** This field is valid if SMF1154_1_PORTRSaf or SMF1154_1_PORTUSaf is set to 1. This field contains the SAF resource name, padded with trailing blanks. Configured with the SAF parameter on the PORT or PORTRANGE statement

Management configuration section

The information that is provided in the management configuration section reflects fields that are configured on the NETMONITOR, SACONFIG, and SMFCONFIG statements in the TCP/IP profile unless otherwise noted.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_MGMTEye	4	EBCDIC	Identifier – 'MGMT'
4(X'4')	SMF1154_1_MGMT119FtpClient	1	Binary	**FTP client SMF 119 records** 0 – FTP client SMF 119 records not requested

Offset	Name	Length	Format	Description
				1 – FTP client SMF 119 records requested Configured with the SMFCONFIG TYPE119 FTPCLIENT / NOFTPCLIENT parameter
5(X'5')	SMF1154_1_MGMT119IfStats	1	Binary	**Interface statistics SMF 119 records** 0 – Interface statistics SMF 119 records not requested 1 – Interface statistics SMF 119 records requested Configured with the SMFCONFIG TYPE119 IFSTATISTICS / NOIFSTATISTICS parameter
6(X'6')	SMF1154_1_MGMT119IPSec	1	Binary	**IPSec SMF 119 records** 0 – IPSec SMF 119 records not requested 1 – IPSec SMF 119 records requested Configured with the SMFCONFIG TYPE119 IPSECURITY / NOIPSECURITY parameter
7(X'7')	SMF1154_1_MGMT119PortStats	1	Binary	**Port statistics SMF 119 records** 0 – Port statistics SMF 119 records not requested 1 – Port statistics SMF 119 records requested Configured with the SMFCONFIG TYPE119 PORTSTATISTICS / NOPORTSTATISTICS parameter
8(X'8')	SMF1154_1_MGMT119Profile	1	Binary	**Profile SMF 119 records** 0 – TCP/IP profile SMF 119 records not requested 1 – TCP/IP profile SMF 119 records requested

Offset	Name	Length	Format	Description
				Configured with the SMFCONFIG TYPE119 PROFILE / NOPROFILE parameter
9(X'9')	SMF1154_1_MGMT119TcpInit	1	Binary	**TCP conn init SMF 119 records** 0 – TCP connection initiation SMF 119 records not requested 1 – TCP connection initiation SMF 119 records requested Configured with the SMFCONFIG TYPE119 TCPINIT / NOTCPINIT parameter
10(X'A')	SMF1154_1_MGMT119TcpipStats	1	Binary	**TCP/IP statistics SMF 119 records** 0 – TCP/IP statistics SMF 119 records not requested 1 – TCP/IP statistics SMF 119 records requested Configured with the SMFCONFIG TYPE119 TCPIPSTATISTICS / NOTCPIPSTATISTICS parameter
11(X'B')	SMF1154_1_MGMT119TcpStack	1	Binary	**Stack init/term SMF 119 records** 0 – TCP/IP stack initiation and termination SMF 119 records not requested 1 – TCP/IP stack initiation and termination SMF 119 records requested Configured with the SMFCONFIG TYPE119 TCPSTACK/ NOTCPSTACK parameter
12(X'C')	SMF1154_1_MGMT119TcpTerm	1	Binary	**TCP conn term SMF 119 records** 0 – TCP connection termination SMF 119 records not requested 1 – TCP connection termination SMF 119 records requested Configured with the SMFCONFIG TYPE119 TCPTERM / NOTCPTERM

Offset	Name	Length	Format	Description
				parameter
13(X'D')	SMF1154_1_MGMT119TN3270Client	1	Binary	**Telnet client init/term SMF 119 records** 0 – TSO Telnet client connection initiation and termination SMF 119 records not requested 1 – TSO Telnet client connection initiation and termination SMF 119 records requested Configured with the SMFCONFIG TYPE119 TN3270CLIENT / NOTN3270CLIENT parameter
14(X'E')	SMF1154_1_MGMT119UdpTerm	1	Binary	**UDP term SMF 119 records** 0 – UDP endpoint termination SMF 119 records not requested 1 – UDP endpoint termination SMF 119 records requested Configured with the SMFCONFIG TYPE119 UDPTERM / NOUDPTERM parameter
15(X'F')	SMF1154_1_MGMT119Dvipa	1	Binary	**Dynamic VIPA SMF 119 records** 0 – Dynamic VIPA SMF 119 records not requested 1 – Dynamic VIPA SMF 119 records requested Configured with the SMFCONFIG TYPE119 DVIPA / NODVIPA parameter
16(X'10')	SMF1154_1_MGMT119SmcrGrpStats	1	Binary	**SMC-R group stats SMF 119 records** 0 – SMC-R group statistics SMF 119 records not requested 1 – SMC-R group statistics SMF 119 records requested Configured with the SMFCONFIG TYPE119 SMCRGROUPSTATISTICS / NOSMCRGROUPSTATISTICS parameter
17(X'11')	SMF1154_1_MGMT119SmcrL	1	Binary	**SMC-R link event SMF 119 records**

Offset	Name	Length	Format	Description
	nkEvent			0 – SMC-R link event SMF 119 records not requested 1 – SMC-R link event SMF 119 records requested Configured with the SMFCONFIG TYPE119 SMCRLINKEVENT / NOSMCRLINKEVENT parameter
18(X'12')	SMF1154_1_MGMT119SmcdLnkStats	1	Binary	**SMC-D link stats SMF 119 records** 0 – SMC-D link statistics SMF 119 records not requested 1 – SMC-D link statistics SMF 119 records requested Configured with the SMFCONFIG TYPE119 SMCDLINKSTATISTICS / NOSMCDLINKSTATISTICS parameter
19(X'13')	SMF1154_1_MGMT119SmcdLnkEvent	1	Binary	**SMC-D link event SMF 119 records** 0 – SMC-D link event SMF 119 records not requested 1 – SMC-D link event SMF 119 records requested Configured with the SMFCONFIG TYPE119 SMCDLINKEVENT / NOSMCDLINKEVENT parameter
20(X'14')	SMF1154_1_MGMT119ZertDetail	1	Binary	**zERT detail SMF 119 records** 0 – zERT connection details SMF 119 records not requested 1 – zERT connection details SMF 119 records requested Configured with the SMFCONFIG TYPE119 ZERTDETAIL / NOZERTDETAIL parameter
21(X'15')	SMF1154_1_MGMT119ZertSummary	1	Binary	**zERT summary SMF 119 records** 0 – zERT summary information SMF 119 records not requested 1 – zERT summary information SMF 119

Offset	Name	Length	Format	Description
				records requested Configured with the SMFCONFIG TYPE119 ZERTSUMMARY / NOZERTSUMMARY parameter
22(X'16')	V2R4: This field is reserved and set to 0. V2R5 and later: SMF1154_1_MGMT119ZertDtlPolicy	1	Binary	**zERT detail SMF 119 records by policy** 0 – zERT connection details SMF 119 records not requested for use with zERT policy-based enforcement 1 – zERT connection details SMF 119 records requested for use with zERT policy-based enforcement Configured with the SMFCONFIG TYPE119 ZERTDETAILBYPOLICY / NOZERTDETAILBYPOLICY parameter
23(X'17')	SMF1154_1_MGMTNMPktTrace	1	Binary	**NETMONITOR packet trace** 0 – NETMONITOR packet trace (SYSTCPDA) not enabled 1 – NETMONITOR packet trace (SYSTCPDA) enabled Configured with the PKTTRCSERVICE / NOPKTTRCSERVICE parameter on the NETMONITOR statement
24(X'18')	SMF1154_1_MGMTNMTcpConn	1	Binary	**NETMONITOR TCP connection** 0 – NETMONITOR TCP connection (SYSTCPCN) not enabled 1 – NETMONITOR TCP connection (SYSTCPCN) enabled Configured with the TCPCONNSERVICE / NOTCPCONNSERVICE parameter on the NETMONITOR statement
25(X'19')	SMF1154_1_MGMTNMSmf	1	Binary	**NETMONITOR SMF service** 0 – NETMONITOR SMF service (SYSTCPSM) not enabled 1 – NETMONITOR SMF service (SYSTCPSM) enabled

Offset	Name	Length	Format	Description
				Configured with the SMFSERVICE / NOSMFSERVICE parameter on the NETMONITOR statement
26(X'1A')	SMF1154_1_MGMTNMNTATrace	1	Binary	**NETMONITOR OSAENT trace** 0 – NETMONITOR OSAENT trace (SYSTCPOT) not enabled 1 – NETMONITOR OSAENT trace (SYSTCPOT) enabled Configured with the NTATRCSERVICE / NONTATRCSERVICE parameter on the NETMONITOR statement
27(X'1B')	SMF1154_1_MGMTNMZert	1	Binary	**NETMONITOR zERT detail** 0 – NETMONITOR zERT detail service (SYSTCPER) not enabled 1 – NETMONITOR zERT detail (SYSTCPER) enabled Configured with the ZERTSERVICE / NOZERTSERVICE parameter on the NETMONITOR statement
28(X'1C')	SMF1154_1_MGMTNMZertSumm	1	Binary	**NETMONITOR zERT summary** 0 – NETMONITOR zERT summary service (SYSTCPES) not enabled 1 – NETMONITOR zERT summary (SYSTCPES) enabled Configured with the ZERTSUMMARY / NOZERTSUMMARY parameter on the NETMONITOR statement
29(X'1D')	V2R4: This field is reserved and set to 0. V2R5 and later: SMF1154_1_MGMTNMZertSrvP	1	Binary	**NETMONITOR zERT detail by policy** 0 – NETMONITOR zERT detail service (SYSTCPER) not enabled for use with zERT policy-based enforcement 1 – NETMONITOR zERT detail (SYSTCPER) enabled for use with zERT policy-based enforcement

Offset	Name	Length	Format	Description
				Configured with the ZERTSERVICEBYPOLICY / NOZERTSERVICEBYPOLICY parameter on the NETMONITOR statement
30(X'1E')	SMF1154_1_MGMTNMSmfIPSec	1	Binary	**SMFSERVICE IPSec records** 0 – IPSec records not requested 1 – IPSec records requested Configured with the IPSECURITY / NOIPSECURITY parameter on the NETMONITOR SMFSERVICE statement
31(X'1F')	SMF1154_1_MGMTNMSmfProfile	1	Binary	**SMFSERVICE profile records** 0 – Profile records not requested 1 – TCP/IP stack profile records and TN3270 Telnet server (Telnet) profile records requested Configured with the PROFILE / NOPROFILE parameter on the NETMONITOR SMFSERVICE statement
32(X'20')	SMF1154_1_MGMTNMSmfCSSMTP	1	Binary	**SMFSERVICE CSSMTP records** 0 – CSSMTP records not requested 1 – CSSMTP records requested Configured with the CSSMTP / NOCSSMTP parameter on the NETMONITOR SMFSERVICE statement
33(X'21')	SMF1154_1_MGMTNMSmfCSMail	1	Binary	**SMFSERVICE MAIL records** 0 – CSSMTP MAIL records not requested 1 – CSSMTP MAIL records requested Configured with the CSMAIL / NOCSMAIL parameter on the NETMONITOR SMFSERVICE statement
34(X'22')	SMF1154_1_MGMTNMSmfDvipa	1	Binary	**SMFSERVICE DVIPA records** 0 – DVIPA records not requested 1 – DVIPA records requested

Offset	Name	Length	Format	Description
				Configured with the DVIPA / NODVIPA parameter on the NETMONITOR SMFSERVICE statement
35(X'23')	SMF1154_1_MGMTNetMonMinLife	1	Binary	**TCPCONNSERVICE minimum lifetime** This field is valid if SMF1154_1_MGMTNMTcpConn is set to 1. The minimum connection lifetime, specified in seconds, for connections reported by the TCP connection information service (TCPCONNSERVICE). Configured with the MINLIFETIME parameter on the NETMONITOR TCPCONNSERVICE statement
36(X'24')	SMF1154_1_MGMTSAEnabled	1	Binary	**TCP/IP SNMP subagent enabled** 0 – TCP/IP SNMP subagent not enabled 1 – TCP/IP SNMP subagent enabled Configured with the ENABLED or DISABLED parameters on the SACONFIG statement
37(X'25')	SMF1154_1_MGMTSASetsEnabled	1	Binary	**SNMP SET requests enabled** This field is valid if SMF1154_1_MGMTSAEnabled is set to 1. 0 – TCP/IP SNMP subagent does not process SNMP SET requests 1 – TCP/IP SNMP subagent processes SNMP SET requests Configured with the SETSENABLED or SETSDISABLED parameters on the SACONFIG statement
38(X'26')	SMF1154_1_MGMTSACommunity	1	Binary	**Community name configured** This field is valid if

Offset	Name	Length	Format	Description
				SMF1154_1_MGMTSAEnabled is set to 1. 0 – Community name not configured 1 – Community name configured Configured with the COMMUNITY parameter on the SACONFIG statement
39(X'27')		1	Binary	Reserved. Set to 0.
40(X'28')	SMF1154_1_MGMTSAAgent	2	Binary	**SNMP agent port number** This field is valid if SMF1154_1_MGMTSAEnabled is set to 1 SNMP agent port number. The value can be in the range 1 – 65535. Configured with the AGENT parameter on the SACONFIG statement
42(X'2A')	SMF1154_1_MGMTSACacheTime	2	Binary	**TCP/IP SNMP agent cache time** This field is valid if SMF1154_1_MGMTSAEnabled is set to 1 Number of seconds that the TCP/IP subagent caches management data. The value can be from 0 – 3,600. Configured with the SACACHETIME parameter on the SACONFIG statement

Network access configuration section

The information that is provided in a network access configuration section entry reflects fields that are configured on the NETACCESS statement in the TCP/IP profile unless otherwise noted. There can be multiple instances of this section in the record, one per NETACCESS network sub statement.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_NETAEye	4	EBCDIC	Identifier – 'NETA'
4(X'4')	SMF1154_1_NETAIPv6	1	Binary	**NETACCESS IP address family** 0 – IP addresses are IPv4

Offset	Name	Length	Format	Description
				1 – IP addresses are IPv6 Configured on the NETACCESS network sub statement
5(X'5')	SMF1154_1_NETAInBound	1	Binary	**NETACCESS inbound checking** 0 – Inbound network access control checking is not in effect. 1 – Inbound network access control checking is in effect. Configured with the INBOUND / NOINBOUND parameter.
6(X'6')	SMF1154_1_NETAOutBound	1	Binary	**NETACCESS outbound checking** 0 – Outbound network access control checking is not in effect. 1 – Outbound network access control checking is in effect. Configured with the OUTBOUND / NOOUTBOUND parameter.
7(X'7')	SMF1154_1_NETADefault	1	Binary	**NETACCESS DEFAULT entry** 0 – This is not a DEFAULT entry. 1 – This is a DEFAULT entry. Configured with the DEFAULT parameter
8(X'8')	SMF1154_1_NETADefaultHome	1	Binary	**NETACCESS DEFAULTHOME entry** 0 – This is not a DEFAULTHOME entry. 1 – This is a DEFAULTHOME entry. Configured with the DEFAULTHOME parameter
9(X'9')	SMF1154_1_NETANetwPfxLen	1	Binary	**Network address prefix length** Network address prefix length for the IPv4 or IPv6 network value Configured on the NETACCESS network

Offset	Name	Length	Format	Description
				sub statement
10(X'A')	SMF1154_1_NETACache	1	Binary	**NETACCESS cache option** SMF1154_1_NETACacheAll (1) When a SAF call is made to check whether a user has access to a security zone, the result is cached regardless of whether access is permitted or denied. SMF1154_1_NETACachePermit (2) When a SAF call is made to check whether a user has access to a security zone: ● The result is cached if access is permitted ● The result is not cached if access is denied. SMF1154_1_NETACacheSame (3) When a SAF call is made to check whether a user has access to a security zone: ● The result is cached if access is permitted ● The result is not cached if access is denied. In addition, a new SAF call is made for a previously permitted security zone in one of the following situations: ● If the user that is associated with the socket changes. ● If the IP address that is being accessed changes from the IP address in the previous packet that was received or sent over the socket. Configured with the CACHEALL, CACHEPERMIT, or CACHESAME parameter.
11(X'B')		1	Binary	Reserved. Set to 0.
12(X'C')	SMF1154_1_NETASafName	8	EBCDIC	**NETACCESS SAF resource name** SAF resource name, padded with trailing

Offset	Name	Length	Format	Description
				blanks. Configured on the NETACCESS network sub statement
20(X'14')	SMF1154_1_NETANetwAddr4	4	Binary	**Network address** This field is valid if SMF1154_1_NETADefault=0 (not a DEFAULT entry) and SMF1154_1_NETADefaultHome=0 (not a DEFAULTHOME entry). One of the following values: • If the SMF1154_1_NETAIPv6 field is 0, SMF1154_1_NETANetwAddr4 contains the IPv4 network value. The network value is the IPv4 network address ANDed with the prefix length. • If the SMF1154_1_NETAIPv6 field is 1, SMF1154_1_NETANetwAddr6 contains the IPv6 network value. The network value is the IPv6 network address ANDed with the prefix length. Configured on the NETACCESS network sub statement
20(X'14')	SMF1154_1_NETANetwAddr6	16	Binary	

SMF type 1154, subtype 2 – FTP daemon compliance evidence record

The FTP daemon compliance evidence record provides information collected from START parameters, the FTP.DATA data set, and UNIX environment variables.

The data is provided in the following sections:

- FTP daemon general configuration section provides configuration information for values with a fixed length.
- FTP daemon configuration data section provides configuration information for values with a variable length. This section is a set of variable-length entries. Each entry contains the following fields:
  - Total length of the entry
  - Key of the entry to identify the value that the entry represents

– Value

In this section, entries are provided only for statements that are explicitly specified. Use the key field for each entry to determine which statements are included.

1154 subtype 2 specific section, self-defining section

This section defines the additional sections that are included in the record. A triplet is included for each defined section. The triplet includes the offset to the section from the start of the record, the length of a single instance of the section, and the number of instances of the section in the record.

Offset	Name	Length	Format	Description
0(x'00')	SMF1154_2_TRN	2	Binary	Number of triplets (set to 2)
2(x'02')		2		Reserved (set to 0)
4(x'04')	SMF1154_2_S1_Offset	4	Binary	Offset to FTP daemon general configuration section (from the start of the record)
8(x'08')	SMF1154_2_S1_Length	2	Binary	Length of FTP daemon general configuration section
10(x'0A')	SMF1154_2_S1_Number	2	Binary	Number of FTP daemon general configuration sections (set to 1)
12(x'0C')	SMF1154_2_S2_Offset	4	Binary	Offset to FTP daemon configuration data section (from the start of the record)
16(x'10')	SMF1154_2_S2_Length	2	Binary	Length of FTP daemon configuration data section

18(x'12')	SMF1154_2_S2_Number	2	Binary	Number of FTP daemon configuration data sections (set to 1)

FTP daemon general configuration section

This section provides FTP daemon configuration information for values with a fixed length.

Offset	Name	Length	Format	Description
0(x'00')	SMF1154_2_FDCFIdent	4	EBCDIC	Identifier – 'FDCF'
4(x'04')	SMF1154_2_FDCFApplName	8	EBCDIC	**FTP server application name**
12(x'0C')	SMF1154_2_FDCFStartTime	4	Binary	**Time FTP daemon started** (UTC)
16(x'10')	SMF1154_2_FDCFStartDate	4	Binary	**Date FTP daemon started** (UTC)
20(x'14')	SMF1154_2_FDCFPort	2	Binary	**FTP server PORT**
22(x'16')	SMF1154_2_FDCFLowPasvDataPort	2	Binary	**Passive data port range start** 0 – Passive data port range not configured. >0 - Beginning value in port range FTP server is allowed to use as listening data socket port. Configured with the PASSIVEDATAPORTS statement
24(x'18')	SMF1154_2_FDCFHighPasvDataPort	2	Binary	**Passive data port range end** 0 – Passive data port range not configured. >0 - Ending value in port range FTP server is allowed to use as listening

				data socket port. Configured with the PASSIVEDATAPORTS statement
26(x'1A')		1		Reserved, set to 0
27(x'1B')	SMF1154_2_FDCFAnonSysHFS	1	Binary	**Anonymous user access to z/OS UNIX files** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. 0 – Do not allow anonymous users access to z/OS UNIX System Services files. 1 – Allow anonymous users access to z/OS UNIX System Service files. Configured with the ANONYMOUSFILEACCESS statement
28(x'1C')	SMF1154_2_FDCFAnonSysMVS	1	Binary	**Anonymous user access to MVS data sets** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. 0 - Do not allow anonymous users access to MVS data sets. 1 - Allows anonymous users access to MVS data sets. Configured with the ANONYMOUSFILEACCESS statement
29(x'1D')	SMF1154_2_FDCFAnonFTJES	1	Binary	**Anonymous user access to JES mode** This field is only valid if

				SMF1154_2_FDCFAnonLevel = 3. 0 - Anonymous users cannot access FTP JES mode 1 – Anonymous users can access FTP JES mode Configured with ANONYMOUSFILETYPEJES statement
30(x'1E')	SMF1154_2_FDCFAnonFTSEQ	1	Binary	**Anonymous user access to SEQ mode** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. 0 - Anonymous users cannot access FTP SEQ mode 1 – Anonymous users can access FTP SEQ mode Configured with ANONYMOUSFILETYPESEQ statement
31(x'1F')	SMF1154_2_FDCFAnonFTSQL	1	Binary	**Anonymous user access to SQL mode** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. 0 - Anonymous users cannot access FTP SQL mode 1 – Anonymous users can access FTP SQL mode Configured with ANONYMOUSFILETYPESQL statement
32(x'20')	SMF1154_2_FDCFAnonUser	8	EBCDIC	**Anonymous logon user ID** If anonymous logon is not allowed,

				the value is blanks. Otherwise, the value is the SAF identity that is assigned to the anonymous user. Configured with the ANONYMOUS statement *userid* value or set to 'ANONYMO' if the ANONYMOUS statement is configured without a userid.
40(x'28')	SMF1154_2_FDCFAnonPass	1	Binary	**Anonymous logon password configured** 0 – Anonymous logon is not configured with userid/password 1 – Anonymous logon is configured with userid/password Configured with the *password* value on the ANONYMOUS statement
41(x'29')	SMF1154_2_FDCFAnonSurr	1	Binary	**Anonymous logon configured with SURROGATE option** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. 0 – Anonymous logon is not configured with userid/SURROGATE 1 – Anonymous logon is configured with userid/SURROGATE Configured with the SURROGATE value on the ANONYMOUS statement
42(x'2A')		6		Reserved, set to 0
48(x'30')	SMF1154_2_FDCFAnonHFSDirM	4	Binary	**z/OS Unix mode bits for directories created by anonymous users**

				This field is only valid if SMF1154_2_FDCFAnonLevel = 3. The three octal digits describe the mode bits used for z/OS UNIX directories that are created by anonymous users Configured with the ANONYMOUSHFSDIRMODE statement
52(x'34')	SMF1154_2_FDCFAnonHFSFileM	4	Binary	**z/OS Unix mode bits for files created by anonymous users** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. The three octal digits describe the mode bits used for z/OS UNIX files that are created by anonymous users Configured with the ANONYMOUSHFSFILEMODE statement.
56(x'38')	SMF1154_2_FDCFAnonLevel	1	Binary	**Anonymous level** Type of access permitted to users logged in as an anonymous user. Levels 1, 2, and 3 are defined. Configured with the ANONYMOUSLEVEL statement
57(x'39')	SMF1154_2_FDCFAnonFTPLog	1	Binary	**FTP server activity logged for anonymous user** 0 – FTP server does not log activity for an anonymous user 1 – FTP server logs activity for an anonymous user Configured with the

				ANONYMOUSFTPLOGGING statement
58(x'3A')	SMF1154_2_FDCFAccErrMsg	1	Binary	**Detailed logon failure replies sent to client** 0 – FTP server does not send detailed login failure replies 1 – FTP server sends detailed login failure replies Configured with the ACCESSERRORMSGS statement
59(x'3B')	SMF1154_2_FDCFDebugOnSite	1	Binary	**SITE DEBUG command accepted** 0 – FTP server does not accept a SITE DEBUG command 1 – FTP server accepts SITE DEBUG command to change the general trace options for the current session Configured with the DEBUGONSITE statement
60(x'3C')	SMF1154_2_FDCFDumpOnSite	1	Binary	**SITE DUMP command accepted** 0 – FTP server does not accept a SITE DUMP command 1 – FTP server accepts a SITE DUMP command to change the extended trace options Configured with the DUMPONSITE statement
61(x'3D')	SMF1152_2_FDCFPassPhrase	1	Binary	**Passphrase login allowed** 0 – FTP server does not allow an FTP client to login with a password phrase 1 – FTP server allows an FTP client

				to login with a password phrase Configured with the PASSPHRASE statement
62(x'3E')	SMF1154_2_FDCFPortEntry4	1	Binary	**Resource profile class for login** 0 (TERMINAL) – Use the TERMINAL class with the IPv4 address 1 (SERVAUTH) – Use SERVAUTH class resource if the IPv4 client address is mapped into a network security zone by a NETACCESS statement, otherwise use the TERMINAL class with the IPv4 client address Configured with the PORTOFENTRY4 statement
63(x'3F')	SMF1152_2_FDCFSecImpZos	1	Binary	**TLS handshake timing for implicit secure ports** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) 0 - FTP server expects the TLS handshake before it sends the initial reply 220 1 – FTP server expects the TLS handshake to occur after it sends the initial reply 220 Configured with the SECUREIMPLICITZOS statement
64(x'40')	SMF1154_2_FDCFSMFType119	1	Binary	**FTP server SMF 119 records** 0 - FTP server SMF type 119 records are not requested 1 – All FTP server SMF type 119

				records are requested Configured with the SMF TYPE119 statement
65(x'41')	SMF1154_2_FDCFSMFJes119	1	Binary	**FTP server SMF 119 records when FILETYPE JES** 0 – FTP server SMF type 119 records are not requested when FILETYPE JES 1 – FTP server SMF type 119 records are requested when FILETYPE JES Configured with the SMFJES TYPE119 statement
66(x'42')	SMF1154_2_FDCFSMFSql119	1	Binary	**FTP server SMF 119 records when FILETYPE SQL** 0 – FTP server SMF type 119 records are not requested when FILETYPE SQL 1 – FTP server SMF type 119 records are requested when FILETYPE SQL Configured with the SMFSQL TYPE119 statement
67(x'43')	SMF1154_2_FDCFSMFAppe119	1	Binary	**FTP server SMF 119 append records** 0 - SMF type 119, subtype 70 append records are not requested 1 – SMF type 119, subtype 70 append records are requested Configured with the SMFAPPE or SMF TYPE119 statement

68(x'44')	SMF1154_2_FDCFSMFDcfg119	1	Binary	**FTP server SMF 119 configuration records** 0 – SMF type 119, subtype 71 configuration records are not requested 1 – SMF type 119, subtype 71 configuration records are requested Configured with the SMFDCFG or SMF TYPE119 statement
69(x'45')	SMF1154_2_FDCFSMFDele119	1	Binary	**FTP server SMF 119 delete records** 0 - SMF type 119, subtype 70 delete records are not requested 1 – SMF type 119, subtype 70 delete records are requested Configured with the SMFDEL or SMF TYPE119 statement
70(x'46')	SMF1154_2_FDCFSMFLogon119	1	Binary	**FTP server SMF 119 logon records** 0 - SMF type 119, subtype 72 logon records are not requested 1 – SMF type 119, subtype 72 logon records are requested Configured with the SMFLOGN or SMF TYPE119 statement
71(x'47')	SMF1154_2_FDCFSMFRen119	1	Binary	**FTP server SMF 119 rename records** 0 - SMF type 119, subtype 70 rename records are not requested 1 – SMF type 119, subtype 70 rename records are requested Configured with the SMFREN or SMF TYPE119 statement

72(x'48')	SMF1154_2_FDCFSMFRetr119	1	Binary	**FTP server SMF 119 retrieve records** 0 - SMF type 119, subtype 70 retrieve records are not requested 1 – SMF type 119, subtype 70 retrieve records are requested Configured with the SMFRETR or SMF TYPE119 statement
73(x'49')	SMF1154_2_FDCFSMFStor119	1	Binary	**FTP server SMF 119 store records** 0 - SMF type 119, subtype 70 store records are not requested 1 – SMF type 119, subtype 70 store records are requested Configured with the SMFSTOR or SMF TYPE119 statement
74(x'4A')	Smf1154_2_FDCFVerifyUser	1	Binary	**FTP server verifies access to SAF SERVAUTH PORT resource** 0 – FTP server does not verify user ID access to SAF SERVAUTH PORT*xxxxx* resource (where *xxxxx* is the port on which the FTP server is listening) 1 – FTP server verifies user ID access to SAF SERVAUTH PORT*xxxxx* resource Configured with the VERIFYUSER statement
75(x'4B')	SMF1154_2_FDCFTlscertcheck	1	Binary	**TLS certificate cross-check** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) 0 – FTP does not perform cross-

				checking of certificates 1 – FTP performs cross-checking to validate that certificates for the control and data connection are the same Configured with the TLSCERTCROSSCHECK statement
76(x'4C')	SMF1154_2_FDCFFTPLogging	1	Binary	**FTP session activity logged** SMF1154_2_FDCF_FTPLogging_FALSE(0) – FTP server does not log session activity SMF1154_2_FDCF_FTPLogging_TRUE (1) – FTP server logs session activity Configured with the FTPLOGGING statement
77(x'4D')	SFM1154_2_FDCFEmailAddrChk	1	EBCDIC	**Email addr checked on anonymous login** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. SMF1154_2_FDCF_EmailAddrChk_NO ('N') – FTP server accepts an anonymous user login without validating the email address that is entered by the FTP client SMF1154_2_FDCF_EmailAddrChk_WARNING ('W') – FTP server generates a warning reply to an anonymous user login if the email address is not valid SMF1154_2_FDCF_EmailAddrChk_FAIL ('F') – FTP server rejects an anonymous user login if the email address is not valid

				Configured with the EMAILADDRCHECK statement
78(x'4E')	SMF1154_2_FDCFPasvDataConn	1	EBCDIC	**Verify peer IP address of data socket** SMF1154_2_FDCF_PasvDataConn_UNRESTRICT ('U') – FTP server accepts passive data connection from any IP address SMF1154_2_FDCF_PasvDataConn_NOREDIRECT ('N') – FTP server verifies that the peer address of the data socket is the client's IP address Configured with the PASSIVEDATACONN statement
79(x'4F')	SMF1154_2_FDCFJESIntLevel	1	Binary	**FTP JES interface level** Values are 1 or 2 Configured with the JESINTERFACELEVEL statement
80(x'50')	SMF1154_2_FDCFExt_AUTH_TLS	1	Binary	**TLS enabled** 0 – TLS not enabled for FTP server 1 – TLS enabled for FTP server Configured with the EXTENSIONS AUTH_TLS statement
81(x'51')	SMF1154_2_FDCFExt_AUTH_GSSAPI	1	Binary	**Kerberos enabled** 0 – Kerberos not enabled for FTP server 1 – Kerberos enabled for FTP server Configured with the EXTENSIONS AUTH_GSSAPI statement
82(x'52		2		Reserved, set to 0

')				
84(x'54')	SMF1154_2_FDCFInActive	4	Binary	**Inactivity timeout** FTP control connection inactivity timeout in seconds. The value is in the range of 0 – 86400 seconds. A value of 0 indicates that no inactivity timer is enabled. Configured with the INACTIVE statement
88(x'58')	SMF1154_2_FDCFJESPGTO	4	Binary	**JES PutGet timeout** JES PutGet timeout in seconds. The value is in the range of 0 – 86400. Configured with the JESPUTGETTO statement
92(x'5C')	SMF1154_2_FDCFPortcmd	1	EBCDIC	**PORT / EPRT command accepted** SMF1154_2_FDCF_Portcmd_ACCEPT ('A') – PORT and EPRT commands are accepted by the FTP server SMF1154_2_FDCF_Portcmd_REJECT ('R') – PORT and EPRT commands are rejected by the FTP server Configured with the PORTCOMMAND statement
93(x'5D')	SMF1154_2_FDCFPortcmdIPAddr	1	EBCDIC	**PORT / EPRT IP address restricted** Valid if SMF1154_2_FDCFPortCmd = A SMF1154_2_FDCF_PortcmdIPAddr_NOREDIRECT ('N') – PORT / EPRT command IP address must match the client IP address SMF1154_2_FDCF_PortcmdIPAddr

				_UNRESTRICT ('U') –Any IP address is accepted for the PORT and EPRT commands Configured with the PORTCOMMANDIPADDR statement
94(x'5E')	SMF1154_2_FDCFPortcmdPort	1	EBCDIC	**PORT / EPRT port restricted** Valid if SMF1154_2_FDCFPortCmd = A SMF1154_2_FDCF_PortcmdPort_NOLOWPORTS ('N') – PORT / EPRT rejected if port is less than 1024 SMF1154_2_FDCF_PortcmdPort_UNRESTRICTED ('U') – Any port is accepted for the PORT and EPRT commands Configured with the PORTCOMMANDPORT statement
95(x'5F')	SMF1154_2_FDCFRlySecLevel	1	Binary	**Restrict information in FTP replies** 0 – No restrictions on information that is included in server FTP replies 1 – No IP addresses, hostnames, port numbers, or server operating system level information is included in FTP replies Configured with the REPLYSECURITYLEVEL statement
96(x'60')	SMF1154_2_FDCFSecCtrConn	1	EBCDIC	**Kerberos security level for control connection** Valid if Kerberos is enabled (SMF1154_2_FDCFExt_AUTH_GSSAPI = 1) SMF1154_2_FDCF_SecCtrConn_CLEAR ('C') – Client determines

				whether data is protected and how SMF1154_2_FDCF_SecCtrConn_SAFE ('S') – Data must have integrity protection SMF1154_2_FDCF_SecCtrConn_PRIVATE ('P') - Data must have both integrity and privacy protection Configured with the SECURE_CTRLCONN statement
97(x'61')	SMF1154_2_FDCFSecDataConn	1	EBCDIC	**Security level for data connections (TLS and Kerberos)** Applies to TLS if TLS enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) Applies to Kerberos if Kerberos enabled (SMF1154_2_FDCFExt_AUTH_GSSAPI = 1) SMF1154_2_FDCF_SecDataConn_NEVER ('N') – Server requires data to be transferred with no cipher algorithm applied to the data SMF1154_2_FDCF_SecDataConn_CLEAR ('C') - Client determines whether data is protected and how SMF1154_2_FDCF_SecDataConn_PRIVATE ('P') - For TLS, server requires a cipher algorithm to be applied - For Kerberos, data must have both integrity and privacy protection SMF1154_2_FDCF_SecDataConn_SAFE ('S')

				- For TLS, this is the same as 'P' - For Kerberos, data must have integrity protection, and can also have privacy protection Configured with the SECURE_DATACONN statement
98(x'62')	SMF1154_2_FDCFSecFTP	1	EBCDIC	**Security mechanism required (TLS or Kerberos)** Applies to TLS if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) Applies to Kerberos if Kerberos is enabled (SMF1154_2_FDCFExt_AUTH_GSSAPI = 1) SMF1154_2_FDCF_SecFTP_REQUIRED ('R')– FTP client is required to login using TLS or Kerberos, depending on what is enabled SMF1154_2_FDCF_SecFTP_ALLOWED ('A') – FTP client is allowed but not required to login using TLS or Kerberos Configured with the SECURE_FTP statement
99(x'63')	SMF1154_2_FDCFSecLogin	1	EBCDIC	**Client Authentication (TLS or Kerberos)** Applies to TLS if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) Applies to Kerberos if Kerberos is enabled (SMF1154_2_FDCFExt_AUTH_GSSAPI = 1)

				For TLS, SMF1154_2_FDCF_SecLogin_NOCLIENTAUTH ('N') – No client authentication SMF1154_2_FDCF_SecLogin_REQUIRED ('R') – Server authenticates client certificate SMF1154_2_FDCF_SecLogin_VERIFYUSER ('V') – Certificate's user ID must match the login user ID For Kerberos, the client's ticket is always processed: N – Not applicable R – Not applicable SMF1154_2_FDCF_SecLogin_VERIFYUSER ('V') – User ID in the client's ticket is verified to match the login user ID Configured with the SECURE_LOGIN statement
100(x'64')	SMF1154_2_FDCFSecPSW	1	EBCDIC	**Password required for TLS session** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) SMF1154_2_FDCF_SecPSW_OPTIONAL ('O') - Password is not required for a session protected by TLS if the client provides a certificate that can be used to authenticate the user SMF1154_2_FDCF_SecPSW_REQUIRED ('R') – Password is required for session protected by TLS Configured with the SECURE_PASSWORD statement

101(x'65')	SMF1154_2_FDCFSecPSWKerb	1	EBCDIC	**Password required by Kerberos session** Valid if Kerberos is enabled (SMF1154_2_FDCFExt_AUTH_GSSAPI = 1) SMF1154_2_FDCF_SecPSWKerb_OPTIONAL ('O') - Password is not required for a session protected by Kerberos if the user can be authenticated using a Kerberos ticket SMF1154_2_FDCF_SecPSWKerb_REQUIRED ('R') – Password is required for session protected by Kerberos Configured with the SECURE_PASSWORD_KERBEROS statement
102(x'66')	SMF1154_2_FDCFTLSMec	1	Binary	**TLS mechanism** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) SMF1154_2_FDCF_TLSMec_FTP (0) – TLS is performed by FTP (value no longer set in V2R5 or later) SMF1154_2_FDCF_TLSMec_ATTLS (1) – TLS is performed by ATTLS Configured with the TLSMECHANISM statement
103(x'67')	SMF1154_2_FDCFTLSRfcLevel	1	Binary	**RFC4217 support level** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) SMF1154_2_FDCF_TLSRfcLevel_DR

				AFT (0) - DRAFT level support SMF1154_2_FDCF_TLSRfcLevel_RFC4217 (1) - RFC4217 level support SMF1154_2_FDCF_TLSRfcLevel_CCCNONOTIFY (2) - CCCNONOTIFY (value no longer set in V2R5 or later) Configured with the TLSRFCLEVEL statement
104(x'68')	SMF1154_2_FDCFTLSPort	2	Binary	**Implicit TLS port value** Configured with the TLSPORT statement
106(x'6A')	SMF1154_2_FDCFUmaskstr	3	EBCDIC	**File mode creation mask** Defines which permission bits are not to be set on when a z/OS UNIX file is created Configured with the UMASK statement
109(x'6D')	SMF1154_2_FDCFSecSessReuse	1	EBCDIC	**Secure session reuse** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) SMF1154_2_FDCF_SecSessReuse_ALLOWED ('A') - Session reuse is allowed SMF1154_2_FDCF_SecSessReuse_REQUIRED ('R') - Reusing the FTP control connection's TLS/SSL session is required for subsequent data connections Configured with the SECURE_SESSION_REUSE statement

110(x'6E')		2		Reserved (set to 0)

FTP daemon configuration data section

This section provides FTP daemon configuration information for values with a variable length. This section includes a set of variable-length entries. Entries are provided only for statements that are explicitly configured. Use the key field for each entry to determine which statements are included.

Offset	Name	Length	Format	Description
0(x'00')	SMF1154_2_FDCDIdent	4	EBCDIC	Identifier – 'FDCD'
4(x'04')	SMF1154_2_FDCDItems			Configuration data items. This field consists of a variable number of entries mapped by the SMF1154_2_FDCD_ITEM structure (see Table 7).

Table 7 – FTP daemon configuration section: SMF1154_2_FDCD_ITEM structure

Offset	Name	Length	Format	Description
0(x'00')	SMF1154_2_FDCD_Len	2	Binary	Configuration data length (including the lengths of the SMF1154_2_FDCD_Len and SMF1154_2_FDCD_Key fields)
2(x'02')	SMF1154_2_FDCD_Key	2	Binary	Configuration data key (See Table 8 for possible values)
4(x'04')	SMF1154_2_FDCD_Data	Variable	EBCDIC	Configuration data string

Table 8 – FTP configuration data keys

Data type (SMF1154_2_FDCD_Key values)	Data Length	Format	Description of value in SMF1154_2_FDCD_Data
SMF1154_2_FDCD_ADMAILADDR (1)	1-256	EBCDIC	Email address of the FTP server administrator Configured with the ADMINEMAILADDRESS statement
SMF1154_2_FDCD_ANONHFSINFO (2)	1-256	EBCDIC	z/OS UNIX file mask used to find a z/OS UNIX information file whose contents are displayed when an anonymous user changes directory. The file mask can contain wildcards or can be a full file name. Configured with the ANONYMOUSHFSINFO statement
SMF1154_2_FDCD_ANONLOGMSG (3)	1-1024	EBCDIC	z/OS UNIX file or MVS data set whose contents are displayed when an anonymous user logs in. Configured with the ANONYMOUSLOGINMSG statement
SMF1154_2_FDCD_ANONMVSINFO (4)	1-17	EBCDIC	MVS low-level qualifier (LLQ) used to find an MVS data set whose contents are displayed when an anonymous user changes directory to an MVS data set. The LLQ is appended to the current path. Configured with the ANONYMOUSMVSINFO statement
SMF1154_2_FDCD_BANNER (5)	1-1024	EBCDIC	z/OS UNIX file or MVS data set whose contents are displayed whenever a user connects to FTP. Configured with the BANNER statement
SMF1154_2_FDCD_HFSINFO (6)	1-256	EBCDIC	z/OS UNIX file mask used to find a z/OS UNIX information file whose contents are displayed when a known user changes

			directory. The file mask can contain wildcards or can be a full file name. Configured with the HFSINFO statement
SMF1154_2_FDCD_LOGINMSG (7)	1 – 1024	EBCDIC	z/OS UNIX file or MVS data set whose contents are displayed when a known user logs in. Configured with the LOGINMSG statement
SMF1154_2_FDCD_MVSINFO (8)	1 – 17	EBCDIC	MVS low-level qualifier (LLQ) used to find an MVS data set whose contents are displayed when a known user changes directory to an MVS data set. The LLQ is appended to the current path. Configured with the MVSINFO statement
SMF1154_2_FDCD_BPXK_SETIBMOPT_TRANSPORT (9)	1 – 8	EBCDIC	TCP/IP stack with which the FTP server has stack affinity Configured with the _BPXK_SETIBMOPT_TRANSPORT environment variable
SMF1154_2_FDCD_KRB5_SERVER_KEYTAB (10)	1 – 8	EBCDIC	KRB5_SERVER_KEYTAB environment variable value Configured with the KRB5_SERVER_KEYTAB environment variable

SMF type 1154, subtype 3 - TN3270 Telnet server compliance evidence record

The TN3270E Telnet server compliance evidence record provides information configured in the TN3270E Telnet server profile for a single server port instance. One or more server ports can be configured for a TN3270E Telnet server. A separate record (or set of records) is written for each server port instance.

If the SMF information for a single server port exceeds 32,756 bytes, multiple records are created to provide the complete set of information. In the SMF 1154 common header SMF1154_C_RecordInd indicates if "more records follow" and SMF1154_C_SeqNum indicates the sequence number. The sequence number starts at 0 in the first record and is incremented by 1 with each additional record. SMF1154_C_Correlator provides a correlator value unique to the server port instance.

The triplets in the SMF 1154 subtype 3 specific section indicate which sections (and how many instances of the section) are included in the record.

Records within a set of records can be correlated by using the extended record subtype (SMFHDR1_STP) from the extended SMF header and the system name (SMF1154_C_SystemName), sysplex name (SMF1154_C_SysplexName), jobname (SMF1154_C_Jobname), request ID (SMF1154_C_RequestID), and correlator (SMF1154_C_Correlator) from the SMF 1154 common header.

Each record contains an SMF extended header, an SMF 1154 common triplets section, an SMF 1154 common header section, and an SMF 1154 subtype 3 specific section (self-defining section). The subtype specific section indicates the additional sections that are included in the record.

1154 subtype 3 specific section, self-defining section

This section defines the additional sections that are included in the record. A triplet is included for each defined section. The triplet includes the offset to the section from the start of the record, the length of a single instance of the section, and the number of instances of the section in the record.

Offset	Name	Length	Format	Description
0(x'00')	SMF1154_3_TRN	2	Binary	Number of triplets (set to 8)
2(x'02')		2		Reserved (set to 0)
4(x'04')	SMF1154_3_S1_Offset	4	Binary	Offset to TN3270E Telnet general information section (from the start of the record)
8(x'08')	SMF1154_3_S1_Length	2	Binary	Length of TN3270E Telnet general information section
10(x'0A')	SMF1154_3_S1_Number	2	Binary	Number of TN3270E Telnet general information sections (set to 1)
12(x'0C')	SMF1154_3_S2_Offset	4	Binary	Offset to TelnetGlobals section (from the start of the record)
16(x'10')	SMF1154_3_S2_Length	2	Binary	Length of TelnetGlobals section

18(x'12')	SMF1154_3_S2_Number	2	Binary	Number of TelnetGlobals sections (set to 1)
20(x'14')	SMF1154_3_S3_Offset	4	Binary	Offset to TelnetParms section (from the start of the record)
24(x'18')	SMF1154_3_S3_Length	2	Binary	Length of TelnetParms section
26(x'1A')	SMF1154_3_S3_Number	2	Binary	Number of TelnetParms sections (set to 1)
28(x'1C')	SMF1154_3_S4_Offset	4	Binary	Offset to ParmsGroup section (from the start of the record)
32(x'20')	SMF1154_3_S4_Length	2	Binary	Length of ParmsGroup section
34(x'22')	SMF1154_3_S4_Number	2	Binary	Number of ParmsGroup sections
36(x'24')	SMF1154_3_S5_Offset	4	Binary	Offset to ParmsMap section (from the start of the record)
40(x'28')	SMF1154_3_S5_Length	2	Binary	Length of ParmsMap section
42(x'2A')	SMF1154_3_S5_Number	2	Binary	Number of ParmsMap sections
44(x'2C')	SMF1154_3_S6_Offset	4	Binary	Offset to LUMap sections (from the start of the record)
48(x'30')	SMF1154_3_S6_Length	2	Binary	Length of LuMap section
50(x'32')	SMF1154_3_S6_Number	2	Binary	Number of LuMap sections
52(x'34')	SMF1154_3_S7_Offset	4	Binary	Offset to PrtMap section (from the start of the record)
56(x'38')	SMF1154_3_S7_Length	2	Binary	Length of PrtMap section
58(x'3A')	SMF1154_3_S7_Number	2	Binary	Number of PrtMap sections
60(x'3C')	SMF1154_3_S8_Offset	4	Binary	Offset to RestrictAppl section (from the start of the record)

64(x'40')	SMF1154_3_S8_Length	2	Binary	Length of RestrictAppl section
66(x'42')	SMF1154_3_S8_Number	2	Binary	Number of RestrictAppl sections

TN3270E Telnet server general information section

This section provides general TN3270E Telnet server values. Only one of these sections exists in the record.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNPIIdent	4	EBCDIC	Identifier – 'TNPI'
4(X'4')	SMF1154_3_TNPIStartStck	8	Binary	**Time TN3270E Telnet server was started** (TOD clock value)
12(X'C')	SMF1154_3_TNPIStartDate	4	Packed	**Date TN3270E Telnet was started**

TN3270E Telnet server TelnetGlobals section

This section provides TN3270E Telnet profile values that can be set only on a TelnetGlobals statement. Only one of these sections exists in the record.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNTGIdent	4	EBCDIC	Identifier – 'TNTG'
4(X'4')	SMF1154_3_TNTGSMFProfile	1	Binary	**Profile SMF 119 records** 0 – TN3270E Telnet profile SMF 119 records not requested 1 – TN3270E Telnet profile SMF 119 records requested Configured with the SMFPROFILE / NOSMFPROFILE parameter
5(X'5')	SMF1154_3_TNTGSMF_GrpDtl	1	Binary	**Profile SMF 119 records GroupDetail** Valid if SMF1154_3_TNTGSMFProfile = 1 0 – TN3270E Telnet profile SMF 119 records with GROUPDETAIL not requested

				1 – TN3270E Telnet profile SMF 119 records with GROUPDETAIL requested Configured with the SMFPROFILE GROUPDETAIL / NOGROUPDETAIL parameter
6(X'6')	SMF1154_3_TNTGSAEnable	1	Binary	**SNMP subagent enabled** 0 – SNMP subagent disabled 1 – SNMP subagent enabled Configured with the TNSACONFIG ENABLED / DISABLED parameter
7(X'7')	SMF1154_3_TNTGSACommName	1	Binary	**SNMP Community name configured** Valid if SMF1154_3_TNTGSAEnable = 1. 0 – Community name "public" used 1 – Community name configured to value other than public Configured with the TNSACONFIG COMMUNITY parameter
8(X'8')	SMF1154_3_TNTGSAPort	2	Binary	**SNMP agent port** Valid if SMF1154_3_TNTGSAEnable = 1. Configured with the TNSACONFIG AGENT parameter
10(X'A')	SMF1154_3_TNTGTCPName	8	EBCDIC	**TCP/IP stack name** TCP/IP stack name, if the TN3270 Telnet server has affinity to a specific TCP/IP stack Otherwise, set to blanks Configured with the TCPIPJOBNAME / NOTCPIPJOBNAME parameter

Common parameters structure

The common parameters structure is included in the TelnetParms and ParmsGroup sections. It begins at the same offset within each section.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TPCCConn	1	Binary	**Check client connections** SMF1154_3_TPCCConn_Chk (1) – Check connectivity of pre-existing connections when establishing a new connection with the same client identifier SMF1154_3_TPCCConn_NoChk (2) – Do not check connectivity of pre-existing connections when establishing a new connection with the same client identifier SMF1154_3_TPCCConn_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the CHECKCLIENTCONN / NOCHECKCLIENTCONN statement
1(X'1')	SMF1154_3_TPConnT	1	Binary	**Connection type** SMF1154_3_TPCONNT_SSL (1) – Secure, TLS session required for connection SMF1154_3_TPCONNT_NEGTSSL (2) - TN3270 negotiate secure, TLS session required for connection. However, a TN3270 negotiation is done to determine if the client is willing to negotiate a TLS session. If so, a TLS handshake begins. If not, the connection is closed.

Offset	Name	Length	Format	Description
				SMF1154_3_TPCONNT_BASIC (3) - Basic, connection is established without TLS protection SMF1154_3_TPCONNT_ANY (4) – Any, an attempt is made to establish a TLS session. If the attempt fails, the connection is established without TLS protection. SMF1154_3_TPCONNT_NONE (5) - None, client connection requests rejected SMF1154_3_TPCONNT_NA (0) - Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the CONNTYPE statement
2(X'2')	SMF1154_3_TPExpLogon	1	Binary	**Allow express logon using a passticket** SMF1154_3_TPEXPLOGON_ALLOW (1) – Allow express logon using a passticket based on the user's client X.509 certificate SMF1154_3_TPEXPLOGON_NOALLOW (2) – Do not allow express logon using a passticket based on the user's client X.509 certificate SMF1154_3_TPEXPLOGON_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the EXPRESSLOGON / NOEXPRESSLOGON statement

Offset	Name	Length	Format	Description
3(X'3')	SMF1154_3_TPExpLogonMFA	1	Binary	**Allow express logon using an MFA token** SMF1154_3_TPEXPLOGONMFA_ALLOW (1) – Allow express logon using a Multi-Factor Authentication (MFA) token based on the user's client X.509 certificate SMF1154_3_TPEXPLOGONMFA_NOALLOW (2) – Do not allow express logon using an MFA token based on the user's client X.509 certificate SMF1154_3_TPEXPLOGONMFA_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the EXPRESSLOGONMFA / NOEXPRESSLOGONMFA statement
4(X'4')	SMF1154_3_TPMFAFallback	1	Binary	**Allow fallback to express logon using a passticket** Valid if SMF1154_3_TPExpLogonMFA=1 SMF1154_3_TPMFAFALLBACK_ALLOW (1) – Allow fallback to express logon using a passticket, if MFA is active, but unavailable SMF1154_3_TPMFAFALLBACK_NOALLOW (2) – Do not allow fallback to express logon using a passticket when MFA is active, but unavailable SMF1154_3_TPMFAFALLBACK_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect

Offset	Name	Length	Format	Description
				Configured with EXPRESSLOGONMFA FALLBACK / NOFALLBACK statement
5(X'5')	SMF1154_3_TPPPhrase	1	Binary	**Passphrase can be accepted on solicitor screen** SMF1154_3_TPPPHRASE_PASSPHRASE (1) – Solicitor screen provides space for a passphrase SMF1154_3_TPPPHRASE_NOPASSPHRASE (2) – Solicitor screen provides space only for a password SMF1154_3_TPPPHRASE_DISPASSPHRASE (3) – Solicitor screen only provides password support SMF1154_3_TPPPHRASE_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the PASSWORDPHRASE / NOPPASSWORDPHRASE / DISABLEPASSWORDPHRASE statement
6(X'6')	SMF1154_3_TPTTLSPort	1	Binary	**Port is used for TLS connections** Valid for TelnetParms SMF1154_3_TPTTLSPORT_SECURE (1) – port is used for connections that are secured with TLS (TTLSPORT) SMF1154_3_TPTTLSPORT_UNSECURE (2) – port is used for unsecured connections (PORT) SMF1154_3_TPTTLSPORT_NA (0) – Value not configured for

Offset	Name	Length	Format	Description
				ParmsGroup, associated TelnetParms value in effect Configured with the PORT or TTLSPORT statement
7(X'7')	SMF1154_3_TPSMFInit119	1	Binary	**TN3270E Telnet SNA Session Initiation SMF 119 records** SMF1154_3_TPSMFINIT119_REQ (1) – TN3270E Telnet SNA Session Initiation SMF 119 records requested SMF1154_3_TPSMFINIT119_NOREQ (2) – TN3270E Telnet SNA Session Initiation SMF 119 records not requested SMF1154_3_TPSMFINIT119_NA (0) - Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the SMFINIT TYPE119 statement
8(X'8')	SMF1154_3_TPSMFTerm119	1	Binary	**TN3270E Telnet SNA Session Termination SMF 119 records** SMF1154_3_TPSMFTERM119_REQ (1) – TN3270E Telnet SNA Session Termination SMF 119 records requested SMF1154_3_TPSMFTERM119_NOREQ (2) – TN3270E Telnet SNA Session Termination SMF 119 records not requested SMF1154_3_TPSMFTERM119_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect

Offset	Name	Length	Format	Description
				Configured with the SMFTERM TYPE119 statement
9(X'9')	SMF1154_3_TPTKOGenLu	1	Binary	**Generic LU takeover** SMF1154_3_TPTKOGENLU_NOTENABLED (1) - Generic LU takeover not enabled (NOTKOGENLU or NOTKO) SMF1154_3_TPTKOGENLU_ENABLED (2) - Generic LU takeover enabled, session not transferred to the taker connection (TKOGENLU) SMF1154_3_TPTKOGENLU_RECON (3) - Generic LU takeover enabled, session transferred to the taker (TKOGENLURECON) SMF1154_3_TPTKOGENLU_NA (0) - Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the TKOGENLU, NOTKOGENLU, TKOGENLURECON, or NOTKO statement
10(X'A')	SMF1154_3_TPTKOSpecLu	1	Binary	**Specific LU takeover** SMF1154_3_TPTKOSPECLU_NOTENABLED (1) - Specific LU takeover not enabled (NOTKOSPECLU or NOTKO) SMF1154_3_TPTKOSPECLU_ENABLED (2) - Specific LU takeover enabled, session not transferred to the taker connection (TKOSPECLU) SMF1154_3_TPTKOSPECLU_RECON (3) - Specific LU takeover enabled, session transferred to the taker (TKOSPECLURECON)

Offset	Name	Length	Format	Description
				SMF1154_3_TPTKOSPECLU_NA (0) - Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the TKOSPECLU, NOTKOSPECLU, TKOSPECLURECON, or NOTKO statement
11(X'B')		1	Binary	Reserved, set to 0
12(X'C')	SMF1154_3_TPInact	1	Binary	**Terminal SNA session inactivity timer** SMF1154_3_TPINACT_ON (1) – Inactivity timer in effect SMF1154_3_TPINACT_OFF (2) – Inactivity timer not in effect SMF1154_3_TPINACT_NA (0) - Inactivity timer not configured for ParmsGroup, associated TelnetParms value in effect Configured with the INACTIVE statement
13(X'D')	SMF1154_3_TPKeepInact	1	Binary	**Session setup inactivity timer** SMF1154_3_TPKEEPINACT_ON (1) – Inactivity timer in effect SMF1154_3_TPKEEPINACT_OFF (2) – Inactivity timer not in effect SMF1154_3_TPKEEPINACT_NA (0) - Inactivity timer not configured for ParmsGroup, associated TelnetParms value in effect Configured with the KEEPINACTIVE

Offset	Name	Length	Format	Description
				statement
14(X'E')	SMF1154_3_TPPrtInact	1	Binary	**Printer inactivity timer** SMF1154_3_TPPRTINACT_ON (1) – Inactivity timer in effect SMF1154_3_TPPRTINACT_OFF (2) - Inactivity timer not in effect SMF1154_3_TPPRTINACT_NA (0) - Inactivity timer not configured for ParmsGroup, associated TelnetParms value in effect Configured using the PRTINACTIVE statement
15(X'F')	SMF1154_3_TPProfInact	1	Binary	**Timer for connections with a non-current profile** SMF1154_3_TPPROFINACT_ON (1) – Inactivity timer in effect SMF1154_3_TPPROFINACT_OFF (2) – Inactivity timer not in effect SMF1154_3_TPPROFINACT_NA (0) - Inactivity timer not configured for ParmsGroup, associated TelnetParms value in effect Configured using the PROFILEINACTIVE statement
16(X'10')	SMF1154_3_TPInactSec	4	Binary	**Terminal SNA session inactivity timeout (in seconds)** Valid if SMF1154_3_TPInact = 1 The timer applies to a KEEPOPEN connection only when an SNA session, with the VTAM application, is active. A connection that has no

Offset	Name	Length	Format	Description
				client-VTAM session activity for the specified time is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the inactivity timer. Configured with the INACTIVE statement
20(X'14')	SMF1154_3_TPKeepInactSec	4	Binary	**Session setup inactivity timeout (in seconds)** Valid if SMF1154_3_TPKeepInact = 1 The timer applies to a KEEPOPEN connection with no active SNA session. A connection that has no client-VTAM activity for the specified time is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the inactivity timer. Configured with the KEEPINACTIVE statement
24(X'18')	SMF1154_3_TPPrtInactSec	4	Binary	**Printer inactivity timeout (in seconds)** Valid if SMF1154_3_TPPrtInact = 1 A printer connection with no client-VTAM activity for the specified time is dropped. The value is in a range of 0 – 99999999. A value of 0 disables the inactivity timer. Configured using the PRTINACTIVE statement
28(X'1C')	SMF1154_3_TPProfInactSec	4	Binary	**Timeout for connections with a non-current profile (in seconds)** Valid if SMF1154_3_TPProfInact = 1

Offset	Name	Length	Format	Description
				A connection that does not have a SNA session for the specified time and that is associated with a non-current profile is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the inactivity timer. Configured using the PROFILEINACTIVE statement
32(X'20')	SMF1154_3_TPMaxRcv	1	Binary	**MaxReceive limit** SMF1154_3_TPMAXRCV_ON (1) – MAXRECEIVE limit in effect SMF1154_3_TPMAXRCV_OFF (2) – MAXRECEIVE limit not in effect SMF1154_3_TPMAXRCV_NA (0) - MAXRECEIVE limit not configured for ParmsGroup, associated TelnetParms value in effect Configured using the MAXRECEIVE statement
33(X'21')	SMF1154_3_TPMaxReqSess	1	Binary	**MaxReqSess limit** SMF1154_3_TPMAXREQSESS_ON (1) –MAXREQSESS limit in effect SMF1154_3_TPMAXREQSESS_OFF (2) – MAXREQSESS limit not in effect SMF1154_3_TPMAXREQSESS_NA (0) - MAXREQSESS limit not configured for ParmsGroup, associated TelnetParms value in effect Configured using the MAXREQSESS statement

Offset	Name	Length	Format	Description
34(X'22')	SMF1154_3_TPMax_RUChain	1	Binary	**MaxRUChain limit** SMF1154_3_TPMAX_RUCHAIN_ON (1) –MAXRUCHAIN limit in effect SMF1154_3_TPMAX_RUCHAIN_OFF(2) – MAXRUCHAIN limit not in effect SMF1154_3_TPMAX_RUCHAIN_NA (0) - MAXRUCHAIN limit not configured for ParmsGroup, associated TelnetParms value in effect Configured using the MAXRUCHAIN statement
35(X'23')	SMF1154_3_TPMaxTcpSendQ	1	Binary	**MaxTCPSendQ limit** SMF1154_3_TPMAXTCPSENDQ_ON (1) –MAXTCPSENDQ limit in effect SMF1154_3_TPMAXTCPSENDQ_OFF (2) – MAXTCPSENDQ limit not in effect SMF1154_3_TPMAXTCPSENDQ_NA (0) - MAXTCPSENDQ limit not configured for ParmsGroup, associated TelnetParms value in effect Configured using the MAXTCPSENDQ statement
36(X'24')	SMF1154_3_TPMaxVtamSendQ	1	Binary	**MaxVTAMSendQ limit** SMF1154_3_TPMAXVTAMSENDQ_ON (1) –MAXVTAMSENDQ limit in effect SMF1154_3_TPMAXVTAMSENDQ_OFF (2) – MAXVTAMSENDQ limit

Offset	Name	Length	Format	Description
				not in effect SMF1154_3_TPMAXVTAMSENDQ_NA (0) - MAXVTAMSENDQ limit not configured for ParmsGroup, associated TelnetParms value in effect Configured using the MAXVTAMSENDQ statement
37(X'25')		3	Binary	**Reserved, set to 0**
40(X'28')	SMF1154_3_TPMaxRcvSize	4	Binary	**Bytes received from client without an EOR** Valid if SMF1154_3_TPMaxRcv = 1 The number of bytes that can be received from a client without an End of Record (EOR) being received. If the amount of data received exceeds the limit, the connection is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the limit check function. Protects against a client in a send-data loop. Configured using the MAXRECEIVE statement
44(X'2C')	SMF1154_3_TPMaxReqSessNum	4	Binary	**Number of session requests received in 10-second period** Valid if SMF1154_3_TPMaxReqSess = 1 Number of session requests that can be received in a 10-second period. If the limit is exceeded, the connection is dropped and an error is reported. The value is in a range of 0 - 99999999. A value of 0 disables the limit check function.

Offset	Name	Length	Format	Description
				Protects against session logon loops that are possibly created by an automatic CLSDST-PASS to an inactive application. Configured using the MAXREQSESS statement
48(X'30')	SMF1154_3_TPMaxRUChainNum	4	Binary	**Number of chained RUs received without an EC** Valid if SMF1154_3_TPMax_RUChain = 1 The number of chained RUs received from an application without an end of chain (EC) being received. If the number of RUs received exceeds the limit, the session, and conditionally the connection, is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the limit check function. This parameter protects against a host application sending too much chained data. Configured using the MAXRUCHAIN statement
52(X'34')	SMF1154_3_TPMaxTcpSndQNum	4	Binary	**Number of bytes queued to be sent to a client** Valid if SMF1154_3_TPMaxTcpSendQ = 1 The number of bytes that are queued to be sent to a client. If the queue size exceeds the limit, the connection is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the limit check function. This parameter prevents large amounts of storage from being held

Offset	Name	Length	Format	Description
				for data that is destined for an unresponsive client. Configured using the MAXTCPSENDQ statement
56(X'38')	SMF1154_3_TPMxVtamSndQNum	4	Binary	**Number of RPLs queued to be sent to VTAM** Valid if SMF1154_3_TPMaxVtamSendQ = 1 The number of data segments (RPLs) queued to be sent to VTAM. If the queue size exceeds the limit, the connection is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the limit check function. This parameter protects against using large amounts of storage to contain data destined for a host VTAM application that is not receiving data. Configured using the MAXVTAMSENDQ statement
60(X'3C')	SMF1154_3_TPNacUserId	8	EBCDIC	**Network access user ID** If not blank, user ID used for network access (NETACCESS) control checking. Otherwise (field is blank), the TN3270E Telnet's address space user ID is used for network access control checking. Configured with the NACUSERID / NONACUSERID statement

TN3270E Telnet server TelnetParms section

This section identifies the server port for which the record is being written. This section provides the profile values that can be set on the TelnetParms statement.

Note: A server port is identified with a port number, a port number and IP address, or a port number and link name.

The TelnetParms section includes a reference to the Common parameters structure.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNTPIdent	4	EBCDIC	Identifier – 'TNTP'
4(X'4')	SMF1154_3_TNTPPortNum	2	Binary	**Port number** Configured with the PORT or TTLSPORT statement
6(X'6')	SMF1154_3_TNTPIndex	2	Binary	**Internal index used by IBM**
8(X'8')	SMF1154_3_TNTPPortIpAddr4	4	Binary	**IPv4 address qualifying port** Valid if SMF1154_3_TNTPPQ_IPaddr = 1 and SMF1154_3_TNTPPQ_IPv6 = 0. Configured with the PORT or TTLSPORT statement
8(X'8')	SMF1154_3_TNTPPortIpAddr6	16	Binary	**IPv6 address qualifying port** Valid if SMF1154_3_TNTPPQ_IPaddr = 1 and SMF1154_3_TNTPPQ_IPv6 = 1. Configured with the PORT or TTLSPORT statement
24(X'18')	SMF1154_3_ TNTPPortLink	16	EBCDIC	**Link name qualifying port** Valid if SMF1154_3_TNTPPQ_Link = 1. Otherwise, set to blanks. Configured with the PORT or TTLSPORT statement
40(X'28')	SMF1154_3_TNTPPQ_Link	1	Binary	**Whether the port is qualified with link name** 0 – Port is not qualified with a link name 1 – Port is qualified with a link name Configured with the PORT or

Offset	Name	Length	Format	Description
				TTLSPORT statement
41(X'29')	SMF1154_3_TNTPPQ_IPaddr	1	Binary	**Whether the port is qualified with IP address** 0 – Port is not qualified with an IP address 1 – Port is qualified with an IP address Configured with the PORT or TTLSPORT statement
42(X'2A')	SMF1154_3_TNTPPQ_IPv6	1	Binary	**IPv6 indicator** This field is valid if the port is qualified with an IP address (SMF1154_3_TNTPPQ_IPaddr = 1). 0 - IPv4 address provided in SMF1154_3_TNTPPortIpAddr4 1 - IPv6 address provided in SMF1154_3_TNTPPortIpAddr6
43(X'2B')		13	Binary	Reserved, set to 0
56(X'38')	SMF1154_3_TNTPCParms	68		See Common parameters structure

TN3270E Telnet server ParmsGroup section

This optional section provides the values of the ParmsGroup statements in the BEGINVTAM block for the server port.

Note: A server port can be identified with a port number, a port number and IP address, or a port number and link name. One entry exists for each ParmsGroup statement for the server port.

The ParmsGroup section includes a reference to the Common parameters structure.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNPGIdent	4	EBCDIC	Identifier – 'TNPG'
4(X'4')	SMF1154_3_TNPGPortNum	2	Binary	**Port number** Port number for the server port instance.
6(X'6')	SMF1154_3_TNPGIndex	2	Binary	**Internal index used by IBM**

Offset	Name	Length	Format	Description
8(X'8')	SMF1154_3_TNPGPortIpAddr4	4	Binary	**IPv4 address qualifying port** Valid if SMF1154_3_TNPGPQ_IPaddr = 1 and SMF1154_3_TNPGPQ_IPv6 = 0. IPv4 address for the server port instance.
8(X'8')	SMF1154_3_TNPGPortIp Addr6	16	Binary	**IPv6 address qualifying port** Valid if SMF1154_3_TNPGPQ_IPaddr = 1 and SMF1154_3_TNPGPQ_IPv6 = 1. IPv6 address for the server port instance.
24(X'18')	SMF1154_3_ TNPGPortLink	16	EBCDIC	**Link name qualifying port** Valid if SMF1154_3_TNPGPQ_Link = 1. Otherwise, set to blanks. Link name for the server port instance.
40(X'28')	SMF1154_3_TNPGPQ_Link	1	Binary	**Whether the port is qualified with link name** 0 – Port is not qualified with a link name 1 – Port is qualified with a link name
41(X'29')	SMF1154_3_TNPGPQ_IPaddr	1	Binary	**Whether the port qualified with IP address** 0 – Port is not qualified with an IP address 1 – Port is qualified with an IP address
42(X'2A')	SMF1154_3_TNPGPQ_IPv6	1	Binary	**IPv6 indicator** This field is valid if the port is qualified with an IP address (SMF1154_3_TNPGPQ_IPaddr = 1).

Offset	Name	Length	Format	Description
				0 - IPv4 address provided in SMF1154_3_TNPGPortIpAddr4 1 - IPv6 address provided in SMF1154_3_TNPGPortIpAddr6
43(X'2B')		5	Binary	Reserved, set to 0
48(X'30')	SMF1154_3_TNPGGroupName	8	EBCDIC	**ParmsGroup name**
56(X'38')	SMF1154_3_TNPGCParms	68		See Common parameters structure

Client ID structure

The client ID structure is included in the ParmsMap, LUMap, and PrtMap sections. The client ID can be one of several types. SMF1154_3_IDType identifies the type of client ID.

The size of the client ID structure is variable. The length of the section in the record must be used to parse the record.

If the client ID structure contains a host name, SMF1154_3_IDHlen contains the length of the host name.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_IDType	1	Binary	**Client ID type** SMF1154_3_ID_EMPTY (0) Unknown type SMF1154_3_ID_USERID (1) SMF1154_3_IDUser is a USERID SMF1154_3_ID_HNAME (2) SMF1154_3_IDHname is a HOSTNAME SMF1154_3_ID_IPADDR (3) SMF1154_3_IDIpAddr*x* is an IPADDR SMF1154_3_ID_USERGRP (4) SMF1154_3_IDGrpName is a USERGRP SMF1154_3_ID_HNGRP (5) SMF1154_3_IDGrpName is

Offset	Name	Length	Format	Description
				an HNGRP SMF1154_3_ID_IPGRP (6) SMF1154_3_IDGrpName is an IPGRP SMF1154_3_ID_DESTIP (7) SMF1154_3_IDIpAddr*x* is a DESTIP SMF1154_3_ID_LNKNAME (8) SMF1154_3_IDLinkName is a LINKNAME SMF1154_3_ID_DIPGRP (9) SMF1154_3_IDGrpName is a DESTIPGRP SMF1154_3_ID_LNKGRP (10) SMF1154_3_IDGrpName is a LINKGRP SMF1154_3_ID_NULL (11) No ID is associated
1(X'1')	SMF1154_3_IDIPv6	1	Binary	**IPv6 indicator** Valid if client identifier is an IP address (SMF1154_3_IDType = 3 or 7) 0 - IPv4 address provided in SMF1154_3_IDIPAddr4 1 - IPv6 address provided in SMF1154_3_IDIPAddr6
1(X'1')	SMF1154_3_IDHlen	1	Binary	**Length of host name** Valid if client identifier is a host name (SMF1154_3_IDType = 2)
2(X'2')	SMF1154_3_IDUser	8	EBCDIC	**User ID** Valid if client identifier is a user ID (SMF1154_3_IDType = 1)
2(X'2')	SMF1154_3_IDLinkName	16	EBCDIC	**Link name** Valid if client identifier is a link name (SMF1154_3_IDType = 8)
2(X'2')	SMF1154_3_IDGrpName	16	EBCDIC	**Group name**

Offset	Name	Length	Format	Description
				Valid if client identifier is group name (SMF1154_3_IDType = 4, 5, 6, 9, or 10)
2(X'2')	SMF1154_3_IDIPaddr4	4	Binary	**IPv4 address** Valid if client identifier is an IPv4 address (SMF1154_3_IDType = 3 or 7 and SMF1154_3_IDIPv6 = 0)
2(X'2')	SMF1154_3_IDIPaddr6	16	Binary	**IPv6 address** Valid if client identifier is an IPv6 address (SMF1154_3_IDType = 3 or 7 and SMF1154_3_IDIPv6 = 1)
2(X'2')	SMF1154_3_IDHName	255	EBCDIC	**Host name** Valid if client identifier is a host name (SMF1154_3_IDType = 2) Note: The length of a host name can be up to 255 bytes. However, SMF1154_3_IDHlen must be used to know the length of the host name.

TN3270E Telnet server ParmsMap section

This optional section provides the values of a ParmsMap statement in the BEGINVTAM block for the server port that is identified in the TelnetParms section. One entry exists for each ParmsMap statement for the server port.

The ParmsMap section includes a reference to a client ID that can be one of several types. See the Client ID structure for the definition of the client ID.

The size of the client ID structure is not fixed. The length of the ParmsMap section in the record must be used to parse the record.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNPMIdent	4	EBCDIC	Identifier – 'TNPM'
4(X'4')	SMF1154_3_TNPMName	8	EBCDIC	ParmsGroup name
12(X'C')	SMF1154_3_TNPMClid			**Client Identifier** See Client ID structure

TN3270E Telnet server LUMap section

This optional section provides the values of an LUMap statement in the BEGINVTAM block for the server port that is identified in the TelnetParms section. One entry exists for each LUMap statement for the server port.

The LUMap section includes a reference to a client ID that can be one of several types. See the Client ID structure for the definition of the client ID.

The size of the client ID structure is not fixed. The length of the LUMap section in the record must be used to parse the record.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNLMIdent	4	EBCDIC	Identifier – 'TNLM'
4(X'4')	SMF1154_3_TNLMName	8	EBCDIC	**LU or LUGroup name**
12(X'C')	SMF1154_3_TNLMPName	8	EBCDIC	**ParmsGroup name** ParmsGroup name if configured. Otherwise, set to blanks. Configured with the PMAP parameter on the LUMAP statement
20(X'14')	SMF1154_3_TNLMClid			**Client Identifier** See Client ID structure

TN3270E Telnet server PrtMap section

This optional section provides the values of a PrtMap statement in the BEGINVTAM block for the server port that is identified in the TelnetParms section. One entry exists for each PrtMap statement for the server port.

The PrtMap section includes a reference to a client ID that can be one of several types. See the Client ID structure for the definition of the client ID.

The size of the client ID structure is not fixed. The length of the PrtMap section in the record must be used to parse the record.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNRMIdent	4	EBCDIC	Identifier – 'TNRM'
4(X'4')	SMF1154_3_TNRMName	8	EBCDIC	**Printer LU or PRTGroup name**
12(X'C')	SMF1154_3_TNRMPName	8	EBCDIC	**ParmsGroup name** ParmsGroup name if configured.

Offset	Name	Length	Format	Description
				Otherwise, set to blanks. Configured with the PMAP parameter on the PRTMAP statement
20(X'14')	SMF1154_3_TNRMClid			**Client Identifier** See Client ID structure

TN3270E Telnet server RestrictAppl section

This optional section provides the values of the RestrictAppl statements in the BEGINVTAM block for the server port that is identified in the TelnetParms section.

Each section includes up to 10 user IDs associated with the RestrictAppl statement. If there are more than 10 user IDs, additional sections are included.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNARIdent	4	EBCDIC	Identifier – 'TNAR'
4(X'4')	SMF1154_3_TNARName	8	EBCDIC	**Application name** The host application name, as specified in VTAMLST. Wild card characters can be included.
12(X'C')	SMF1154_3_TNARCertAuth	1	Binary	**Use derived user ID** 0 – Use RestrictAppl password validation 1 – Use derived user ID based on TLS client certificate, skipping the RestrictAppl password validation Configured with the RestrictAppl CertAuth statement
13(X'D')		3	Binary	Reserved, set to 0
16(X'10')	SMF1154_3_TNARLstCnt	4	Binary	Total number of user IDs defined
20(X'14')	SMF1154_3_TNARLstIdx	4	Binary	Index into user IDs defined
24(X'18')	SMF1154_3_TNARLstNum	4	Binary	Number of user IDs in this section
28(X'1C')	SMF1154_3_TNARLst	80		Array of 10 user IDs
28(X'1C')	SMF1154_3_TNARUser	8	EBCDIC	User ID

SMF type 1154, subtype 4 – CSSMTP client compliance evidence record

The CSSMTP client compliance evidence record provides information that is collected from the CSSMTP configuration file, START parameters, and UNIX environment variables.

The triplets in the 1154 subtype 4 specific section indicate which sections (and how many instances of the section) are included in the record.

1154 subtype 4 specific section, self-defining section

This section defines the additional sections that are included in the record. A triplet is included for each defined section. The triplet includes the offset to the section from the start of the record, the length of a single instance of the section, and the number of instances of the section in the record.

Offset	Name	Length	Format	Description
0(x'00')	SMF1154_4_TRN	2	Binary	Number of triplets (set to 4)
2(x'02')		2		Reserved (set to 0)
4(x'04')	SMF1154_4_S1_Offset	4	Binary	Offset to CSSMTP identification section (from the start of the record)
8(x'08')	SMF1154_4_S1_Length	2	Binary	Length of CSSMTP identification section
10(x'0A')	SMF1154_4_S1_Number	2	Binary	Number of CSSMTP identification sections (set to 1)
12(x'0C')	SMF1154_4_S2_Offset	4	Binary	Offset to CSSMTP configuration section (from the start of the record)
16(x'10')	SMF1154_4_S2_Length	2	Binary	Length of CSSMTP configuration section
18(x'12')	SMF1154_4_S2_Number	2	Binary	Number of CSSMTP configuration sections (set to 1)
20(x'14')	SMF1154_4_S3_Offset	4	Binary	Offset to CSSMTP target server section (from the start of the record)
24(x'18')	SMF1154_4_S3_Length	2	Binary	Length of CSSMTP target server section
26(x'1A')	SMF1154_4_S3_Number	2	Binary	Number of CSSMTP target server sections
28(x'1C')	SMF1154_4_S4_Offset	4	Binary	Offset to CSSMTP configuration data section (from the start of the record)
32(x'20')	SMF1154_4_S4_Length	2	Binary	Length of CSSMTP configuration

				data section
34(x'22')	SMF1154_4_S4_Number	2	Binary	Number of CSSMTP configuration data sections (set to 1)

CSSMTP identification section

This section identifies the CSSMTP client that created this SMF record.

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_4_MLCI_Ident	4	EBCDIC	Identifier - 'MLCI'
4(X'4')	SMF1154_4_MLCI_JMR	24	Structure	**Job Management Record**
4(X'4')	SMF1154_4_MLCI_Job	8	EBCDIC	Jobname
12(X'C')	SMF1154_4_MLCI_Entry	4	Binary	Time since midnight, in hundredths of a second, when CSSMTP was started.
16(X'10')	SMF1154_4_MLCI_EDate	4	Packed	Date when CSSMTP was started, in the form 0cyydddF.
20 (X'14')	SMF1154_4_MLCI_USEID	8	EBCDIC	User-defined identification field (taken from common exit parameter area, not from USER=parameter on job statement).
28 (X'1C')	SMF1154_4_MLCI_ExtWrt	8	EBCDIC	**External writer name** Configured with the ExtWrtName statement.
36(X'24')	SMF1154_4_MLCI_Jes	4	EBCDIC	**JES subsystem name**

CSSMTP configuration section

This section provides configuration settings for this CSSMTP client.

Offset	Name	Length	Type	Description
0(X'0')	SMF1154_4_MLCF_Ident	4	EBCDIC	Identifier – 'MLCF'
4(X'4')	SMF1154_4_MLCF_Tcpip	8	EBCDIC	**TCP/IP stack with which CSSMTP has affinity** TCP/IP stack name if the CSSMTP client has stack affinity. Otherwise, set to blanks. Set from the -p/-P CSSMTP start

Offset	Name	Length	Type	Description
				option.
12(X'C')	SMF1154_4_MLCF_UserInfo	1	Binary	**CSSMTP user information included in mail header** 0 – User information is not inserted into the mail message header by CSSMTP 1 – User information is inserted into the mail message header by CSSMTP Configured with the UserInfo parameter on the Header statement.
13(X'D')	SMF1154_4_MLCF_SmfConf	1	Binary	**CSSMTP configuration SMF 119 records** 0 – CSSMTP configuration SMF 119 records not requested 1 – CSSMTP configuration SMF 119 records requested Configured with the Config parameter on the SMF119 statement.
14(X'E')	SMF1154_4_MLCF_SmfConn	1	Binary	**CSSMTP connection SMF 119 records** 0 – CSSMTP connection SMF 119 records not requested 1 – CSSMTP connection SMF 119 records requested Configured with the Connect parameter on the SMF119 statement.
15(X'F')	SMF1154_4_MLCF_SmfMail	1	Binary	**CSSMTP mail message SMF 119 records** 0 – CSSMTP mail message SMF 119 records not requested 1 – CSSMTP mail message SMF 119 records requested

Offset	Name	Length	Type	Description
				Configured with the Mail parameter on the SMF119 statement.
16(X'10')	SMF1154_4_MLCF_SmfSpool	1	Binary	**CSSMTP spool SMF 119 records** 0 – CSSMTP spool SMF 119 records not requested 1 – CSSMTP spool SMF 119 records requested Configured with the Spool parameter on the SMF119 statement.
17(X'11')	SMF1154_4_MLCF_SmfStats	1	Binary	**CSSMTP statistics SMF 119 records** 0 – CSSMTP statistics SMF 119 records not requested 1 – CSSMTP statistics SMF 119 records requested Configured with the Stats parameter on the SMF119 statement.
18(X'12')	SMF1154_4_MLCF_UserExt	1	Binary	**CSSMTP user exit version** SMF1154_4_MLCF_USEREXIT_NONE (0) - CSSMTP user exit is not configured or is not active SMF1154_4_MLCF_USEREXIT_VERSION2 (2) – CSSMTP user exit uses the exit facility token name EZBTCPIPSMTPEXIT. Only supports RFC 821 mail syntax. SMF1154_4_MLCF_USEREXIT_VERSION3(3) – CSSMTP user exit uses the exit facility token name EZATCPIPCSSMTPV3. Supports both RFC 821 and RFC 2821 mail syntax. Configured with the USEREXIT statement.

Offset	Name	Length	Type	Description
19(X'13')		1		Reserved. Set to 0.

CSSMTP target server section

This section provides configuration settings for a target server that is configured with the TargetServer statement. There can be multiple instances of this section, one for each target server.

Note: More than one target server can be defined with a single TargetServer statement.

Offset	Name(Dim)	Length	Type	Description
0(X'0')	SMF1154_4_MLTS_Ident	4	EBCDIC	Identifier – 'MLTS'
4(X'4')	SMF1154_4_MLTS_Port	2	Binary	**Target server port value** Configured with the ConnectPort parameter on the TargetServer statement.
6(X'6')	SMF1154_4_MLTS_Type	1	Binary	**Type of target server configuration** SMF1154_4_MLTS_TYPE_ADDRESS (0) - Target IP address SMF1154_4_MLTS_TYPE_NAME (1) - Target name SMF1154_4_MLTS_TYPE_MX (2) - Target mail exchange (MX) Configured with the TargetIP, TargetName, or TargetMx parameter on the TargetServer statement.
7(X'7')	SMF1154_4_MLTS_IPv6	1	Binary	**Target IP address IPv6 indicator** This field is valid if a target IP address is configured (SMF1154_4_MLTS_Type = 0). 0 - IPv4 address provided in SMF1154_4_MLTS_IPaddr4 1 - IPv6 address provided in SMF1154_4_MLTS_IPaddr6

Offset	Name(Dim)	Length	Type	Description
8(X'8')	SMF1154_4_MLTS_IPaddr4	4	Binary	**Target IPv4 address** This field is valid if a target IPv4 address is configured (SMF1154_4_MLTS_Type = 0 and SMF1154_4_MLTS_IPv6 = 0). Configured with the TargetIP parameter on the TargetServer statement.
8(X'8')	SMF1154_4_MLTS_IPaddr6	16	Binary	**Target IPv6 address** This field is valid if a target IPv6 address is configured (SMF1154_4_MLTS_Type = 0 and SMF1154_4_MLTS_IPv6 = 1). Configured with the TargetIP parameter on the TargetServer statement.
24(X'18')	SMF1154_4_MLTS_Secure	1	Binary	**TLS support required** Indicates whether Transport Layer Security (TLS) is required between the CSSMTP client and the target server. SMF1154_4_MLTS_SECURE_TLSNO (0) - TLS is not required SMF1154_4_MLTS_SECURE_TLSREQ (1) -TLS is required Note: If the STARTTLS SMTP command is used in the spool file, a TLS connection is attempted with the target server even if SMF1154_4_MLTS_Secure is 0. Configured with the Secure parameter on the TargetServer statement.
25(X'19')		3		Reserved. Set to 0.

CSSMTP configuration data section

This section provides configuration information for CSSMTP client configuration statements with variable-length values. There is one instance of this section with one or more variable-length entries.

The section includes a section identifier and a variable number of entries that are mapped by the SMF1154_4_MLCD_ITEM structure.

Offset	Name	Length	Format	Description
0(x'00')	SMF1154_4_MLCD_Ident	4	EBCDIC	Identifier – 'MLCD'
4(x'04')	SMF1154_4_MLCD_Items			Configuration data items. This field consists of a variable number of entries that are mapped by the SMF1154_4_MLCD_ITEM structure (see Table 9).

Table 9 – CSSMTP configuration data section: SMF1154_4_MLCD_ITEM structure

Each entry includes a length, key, and value. The length is the length of the entry including the length of SMF1154_4_MLCD_Len and SMF1154_4_MLCD_Key. The key identifies the configuration data that is provided in the entry.

Offset	Name	Length	Format	Description
0(x'00')	SMF1154_4_MLCD_Len	2	Binary	Configuration data length (including the lengths of the SMF1154_4_MLCD_Len and SMF1154_4_MLCD_Key fields)
2(x'02')	SMF1154_4_MLCD_Key	2	Binary	Configuration data key (See Table 10 for possible values)
4(x'04')	SMF1154_4_MLCD_Data	Variable	EBCDIC	Configuration data value

Table 10 – CSSMTP configuration data keys

SMF1154_4_MLCD_Key values	Data Length	Format	Description of value in SMF1154_4_MLCD_Data
SMF1154_4_MLCD_DomName (40)	1-256	EBCDIC	Resolver-supplied domain name
SMF1154_4_MLCD_HostName (41)	1-64	EBCDIC	Resolver-supplied host name

SMF1154_4_MLCD_TargSrv1 (42)	1-256	EBCDIC	**Target server 1 value** If the first instance of the target server section is defined as a TargetIP, the data field that is identified with this key contains a text version of the IP address. Otherwise, it contains a target name or target MX name value. Configured with the TargetIP, TargetName, or TargetMx parameter on the TargetServer statement.
SMF1154_4_MLCD_TargSrv2 (43)	1-256	EBCDIC	**Target server 2 value** If the second instance of the target server section is defined as a TargetIP, the data field that is identified with this key contains a text version of the IP address. Otherwise, it contains a target name or target MX name value. Configured with the TargetIP, TargetName, or TargetMx parameter on the TargetServer statement.
SMF1154_4_MLCD_TargSrv3 (44)	1-256	EBCDIC	**Target server 3 value** If the third instance of the target server section is defined as a TargetIP, the data field that is identified with this key contains a text version of the IP address.

			Otherwise, it contains a target name or target MX name value. Configured with the TargetIP, TargetName, or TargetMx parameter on the TargetServer statement.
SMF1154_4_MLCD_TargSrv4 (45)	1-256	EBCDIC	**Target server 4 value** If the fourth instance of the target server section is defined as a TargetIP, the data field that is identified with this key contains a text version of the IP address. Otherwise, it contains a target name or target MX name value. Configured with the TargetIP, TargetName, or TargetMx parameter on the TargetServer statement.

Accounting – SMF records

Installations use Systems Management Facilities (SMF) records for the following reasons:

Performance management

Performance management includes the tasks that are related to verifying that defined service levels are met, and if not, identifying possible causes.

Aggregated information about delivered service, structured by organizational units (for which service levels have been defined) is needed to perform these tasks. These reports are typically time series with varying levels of time intervals, ranging from weeks through days to a time interval that matches the SMF interval. Some examples of potential reports related to performance management are:

- TCP connection elapsed time per server port number per time of day (potentially broken down on source IP address, or netmask)
- Number of TCP connections per server port number per time of day (potentially broken down on source IP address, or netmask)
- Number of inbound/outbound bytes transferred in TCP connections per time of day (potentially broken down in various ways: per destination or source port, per destination IP address, netmask, or in total, etc.)
- TCP retransmission activity per time of day (potentially broken down per destination IP address, or netmask)
- Number of outbound TCP connections per time of day (potentially broken down per destination IP address, or netmask)
- Number of inbound/outbound UDP datagrams per time of day (potentially broken down on server port number)
- Number of discards, error packets, and unknown protocol packets inbound and outbound per time of day (potentially broken down per interface)

Capacity planning

Capacity planning includes tasks that are related to forecasting capacity in terms of central processing power, memory, channel-based I/O subsystem, network attachments, and network bandwidth. Such planning tasks are based on analyzing trends for use of capacity during a preceding period (typically one to two years), and applying forecasting metrics, along with knowledge about planned launches of new applications or use of existing applications, to this trend in order to predict capacity needs during the next one to two year period. Some examples of potential reports related to capacity planning are:

- Total number of TCP connections per reserved server port number per day including analysis of average and variations around average during daily peak periods

- Total number of UDP inbound/outbound UDP datagrams per reserved server port number per day including average and variations around average during daily peak periods
- Number of bytes and/or packets transferred inbound and outbound per interface (LINK) per time of day (potentially broken down into unicasts, broadcasts, and multicasts)
- Size of queue length per interface per time of day

Auditing

Auditing involves tasks that are related to identifying and proving that individual events have taken place. Some examples of potential reports related to auditing are:

- Detailed information about specific TCP connections or UDP sockets, IP addresses, server/client identification, duration, number of bytes, and so on
- Details about activity that involves a specific client or server
- Details about a given application session based on server-specific SMF recording, such as individual Telnet sessions or FTP sessions
- Details about changes to the TCP/IP stack profile and the user that requested the change
- Details about changes to the status of dynamic virtual IP addresses (DVIPAs) and sysplex distributor targets

Compliance

Compliance involves tasks that are related to identifying that certain standards (such as PCI-DSS) are met. The SMF 1154 record is designed to capture compliance evidence from many MVS components and applications. TCP/IP provides specific compliance evidence that can be used in conjunction with other SMF 1154 records to evaluate a system's compliance with one or more standards.

Some examples of potential reports related to compliance are:

- TCP/IP stack configured security settings, such as whether AT-TLS and IPsec are enabled
- Application-level compliance information specific to each individual application, for example:
  - For CSSMTP: Configured security settings, such as TLS protection
  - For FTP: Configured security settings, such as anonymous logon support
  - For TN3270: Configured security settings, such as inactivity timeout values

Accounting

Accounting involves tasks that are related to calculating how much each individual user or organizational unit should be charged for use of the shared central IS resources. Input to such calculations vary, but is often based on CPU cycle use, data quantities, bandwidth usage, and memory use. For TCP/IP additional metrics may be defined, such as type of service used (FTP, LPD, web server, and so on), and TCP connection-related information (number of connections,

duration, byte transfer counts, and so on). Some examples of potential reports related to accounting are:

- Aggregated number of connections to a given server from a given source in terms of a specific client IP address, or netmask
- Accumulated connect time to a given server from a given source in terms of a specific client IP address, or netmask.
- Number of bytes transferred to or from a given source in terms of a specific client IP address, or netmask.
- Amount of data protected by specific manual or dynamic tunnels.
- Application-level accounting information specific to each individual server, for example:
  - For Communications Server SMTP (CSSMTP): Information about mail message processing
  - For FTP: Number of transfer operations and bytes retrieved or stored per user ID
  - For IKED: Information about IKE tunnels
  - For TN3270: Number of sessions and session type (TN3270/TN3270E/LINEMODE)

In general, SMF records are created for deferred processing and analysis and are not used for real-time monitoring purposes. In a TCP/IP environment, real-time monitoring is implemented with the SNMP protocol and is based on internal variables that SNMP subagents maintain. However, on z/OS®, much of the information that is written in SMF records is also useful from a real-time monitoring perspective. For information about using z/OS Communications Server TCP/IP network management interfaces (NMIs) to obtain SMF records in real time, see z/OS Communications Server: IP Programmer's Guide and Reference.

As can be seen, all disciplines require detailed data as input. Depending on the discipline, certain levels of aggregation is performed on the raw detailed data in order to perform the tasks of that discipline. The objective of the TCP/IP product is to define and generate the lowest level of detail that is needed by all disciplines. How to aggregate and the actual aggregation is performed by other products, such as Performance Reporter for z/OS (PR), MVS™ Information Control System (MICS), or SAS-based tools or, in many cases, customer-written programs.

TCP/IP– produced SMF records should not be viewed isolated. Other components in MVS produce SMF records for the same purposes as those produced by TCP/IP. An installation is likely to combine information from a series of subsystems in performing detailed performance or capacity planning, or compliance evaluation. SMF records with information about use of CPU resources and memory resources per address space is, for example, produced by other components in MVS, and TCP/IP produced SMF records should not duplicate that information. Also, compliance with a standard (for example, PCI-DSS) requires data from many components in MVS and various applications.

The events that trigger SMF records to be written and the information included in the SMF records must accommodate the intended purposes. There can be multiple purposes for given SMF records.

SMF records can be cut at multiple levels in the TCP/IP protocol stack, and the type of information that can be included depends on where the SMF record is created:

- At the IP and interface layer, there is information about ICMP activity, IP packet fragmentation and reassembly activity, IP checksum errors, IGMP activity, and ARP activity. At this layer, it is difficult to relate the information to specific users (remote clients, local socket address spaces, and so on), so from an accounting point of view, this information is not very interesting. Because you can aggregate network-layer activity to physical interfaces, the information at the IP and interface layer is an important aspect of both performance and capacity management.
- At the transport protocol layer, there is information about IP addresses, port numbers, and host names. For TCP-related workload, there is information about connections and information that is related to TCP connections, such as byte counts, connection times, reliability metrics, and performance metrics. For UDP-related workload, each UDP datagram is a separate entity; the only way to aggregate information for UDP is on a UDP socket level, where SMF records could be created every time a UDP socket is closed.
- At the application layer, there are more details about what goes on, but every application is different and requires separate SMF record definitions and ability to write the SMF records to implement application-layer SMF recording. Application-layer SMF recording is implemented by some applications, such as the TN3270E Telnet server (Telnet), the FTP server, the IKE daemon, and the CSSMTP daemon.

For more information about the SMF records provided by z/OS Communications Server functions, see SMF records in z/OS Communications Server: IP Programmer's Guide and Reference.

TRADEMARKS