System z10

Open Systems Adapter-Express3 Integrated Console Controller Dual-Port User's Guide

SA23-2266-02

System z10

Open Systems Adapter-Express3 Integrated Console Controller Dual-Port User's Guide

SA23-2266-02

Notice

Before using this information and the products it supports, read the information in "Notices" on page 79. You should also familiarize yourself with the *zEnterprise 196, System z10, System z9 and eServer zSeries Open Systems Adapter-Express Customer's Guide and Reference*, SA22–7935, *Hardware Management Console Operations Guide*, SC28-6830, and *System z10 Enterprise Class Support Element Operations Guide, Version 2.10.0*, SC28-6868.

This edition, SA23-2266-02, refers to the IBM Open Systems Adapter-Express3 Integrated Console Controller for the following operating systems: z/OS Version 1 Release 2 or higher (5694-A01), and z/OS.e Version 1 Release 3 or higher (5655-G52), Open Systems Adapter Support Facility for z/Virtual Machine/Enterprise (z/VM) Version 3 Release 1, Version 4 Release 2 (Program Number 5654-A17), and Version 4 Release 3 or higher (Program Number 5739-A03), OSA/SF for VSE Version 2 Release 2 (part of VSE Central Functions 6.1.1, 5686-066) in VSE/ESA Version 2 Release 2.6 (5690-VSE) or higher, and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters. This edition replaces SA23-2266-01.

There may be a newer version of this document in PDF format available on **Resource Link**. Go to

https://www.ibm.com/servers/resourcelink

and click on **Library** on the navigation bar. A newer version is indicated by a lower case, alphabetic letter following the form number suffix (for example: 00a, 00b, 01a, 01b).

Contents

Figures

Tables

About this publication

This document describes the configuration process for the Open Systems Adapter-Express3 Integrated Console Controller Dual-Port.

Who should use this publication

This document is intended for the technical staff who will configure the Open Systems Adapter-Express3 Integrated Console Controller Dual-Port.

What is included in this publication

This publication contains the following chapters and appendixes:

- Chapter 1, "Open Systems Adapter-Express3 Integrated Console Controller overview," on page 1 is an introduction to the Open Systems Adapter-Express Integrated Console Controller.
- Chapter 2, "Dual-port connection rules," on page 5 summarizes the rules for defining either or both physical ports and clients (sessions) during OSA-ICC dual-port configuration.
- Chapter 3, "Defining your OSA-ICC configuration," on page 9 describes how to define your OSA-ICC configuration.
- Chapter 4, "Controlling and configuring an OSA-ICC," on page 15 describes the tasks for configuring your Open Systems Adapter-Express Integrated Console Controllers.
- Chapter 5, "OSA-ICC programming considerations," on page 55 provides brief programming tips for 3270 client support.
- Chapter 6, "eNetwork Personal Communications Configuration," on page 57 provides an example of defining a PCOMM 3270 session.
- Chapter 7, "Error and warning messages," on page 61 describes errors and warnings issued from the validate source file and validate panels.
- Appendix A, "Network topology diagrams," on page 71 describes three network topology diagrams.

Related publications

Important

Please ensure that you are using the most recent version of all related documentation.

Other IBM publications that you will find helpful and that you should use along with this publication include:

- 2074 Usage Tips, GM13–0316.
- IOCP User's Guide for ICP IOCP, SB10–7037

A note on terminology

Throughout this publication, certain equipment terms and short versions of product names are used to make the information more easily understood. These are:

CS Communications Server

1000Base-T
1000Base-T Ethernet feature capable of 10, 100, or 1000 Mbps

GbE Gigabit Ethernet feature

OSA Abbreviation for Open Systems Adapter. This document deals exclusively with the OSA-Express3 features and may refer to OSA-Express3 as OSA.

OSA-Express3
Abbreviation for Open Systems Adapter-Express3 features.

OSA-ICC
Abbreviation for Open Systems Adapter-Express Integrated Console Controller features.

OSC The channel type name for OSA-Express features that are configured as Open Systems Adapter-Express Integrated Console Controller.

OSD The channel type name for OSA-Express features that run under Queued Direct Input/Output architecture (QDIO).

OSE The channel type name for OSA-Express features that do not use QDIO architecture (typically SNA/APPN/HPR applications).

OSN The channel type name for OSA-Express3 features that use QDIO architecture and CDLC protocol.

PCOMM
The Host Access Client Package which includes the eNetwork Personal Communications V5.6 emulator.

How to send your comments to IBM

We appreciate your input on this publication. Feel free to comment on the clarity, accuracy, and completeness of the information or give us any other feedback that you might have.

Use one of the following methods to send us your comments:

1. Send an email to mhvrcfs@us.ibm.com
2. Visit the Contact z/OS web page at http://www.ibm.com/systems/z/os/zos/webqs.html
3. Mail the comments to the following address:
   IBM Corporation
   Attention: MHVRCFS Reader Comments
   Department H6MA, Building 707
   2455 South Road
   Poughkeepsie, NY 12601-5400
   U.S.A.
4. Fax the comments to us as follows:
   From the United States and Canada: 1+845+432-9405
   From all other countries: Your international access code +1+845+432-9405

Include the following information:

- Your name and address
- Your email address
- Your telephone or fax number
- The publication title and order number:
  System z10 Open Systems Adapter-Express3 Integrated Console Controller Dual-Port User's Guide
  SA23-2266-01
- The topic and page number related to your comment
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you submit.

If you have a technical problem

Do not use the feedback methods listed above. Instead, do one of the following:

- Contact your IBM service representative
- Call IBM technical support
- Visit the IBM support portal at www.ibm.com/systems/z/support/

Summary of changes

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

You may notice changes in the style and structure of some content. For example, text that has a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

The "Readers' Comments - We'd Like to Hear from You" section at the back of this publication has been replaced with a new section “How to send your comments to IBM” on page xi. The hardcopy mail-in form has been replaced with a page that provides information appropriate for submitting readers comments to IBM.

Summary of changes for SA23-2266-02

This document contains information that was previously presented in *System z10 Open Systems Adapter-Express3 Integrated Console Controller Dual-Port User's Guide*, SA23-2266-01. The following sections summarize the changes to that information.

Changed Information

This edition includes changed information:

- For OSA-ICC error code 1212, changed the read timeout value range from 0-300 to 5-300.

Summary of changes for SA23-2266-01

This document contains information that was previously presented in *System z10 Open Systems Adapter-Express3 Integrated Console Controller Dual-Port User's Guide*, SA23-2266-00. The following sections summarize the changes to that information.

Changed Information

This edition includes changed information:

- Changed the Device range of 1-65535 to 0-65535.

Summary of changes for SA23-2266-00

This is the initial release of the document.

Chapter 1. Open Systems Adapter-Express3 Integrated Console Controller overview

The IBM® Open Systems Adapter-Express Integrated Console Controller (OSA-ICC) is the replacement for 2074 Console Support Controller and local, non-SNA DFT 3174 Control Units. Its primary application is to provide connectivity, the network performance path is provided by OSD and QDIO modes. The OSA-ICC 3270 sessions allow you to IPL your logical partitions within any channel subsystem (CSS) and to provide System Operator/Master consoles for z/OS®, z/OS.e, z/VM®, TPF, and VSE. These sessions can also be used by TSO, VM, or VSE system programmers.

Throughout this document **OSA-Express3** may be referred to as **OSA**.

Each OSA-ICC is capable of handling 120 sessions. The OSA-ICC uses TCP/IP connections over Ethernet LAN to attach to personal computers (PCs) which are running an RFC 2355 compliant TN3270E emulator.

IBM has tested the Host Access Client Package which includes the eNetwork Personal Communications V5.6 emulator (PCOMM) in CSD3 running under Microsoft Windows XP + for compatibility, however there is no reason to believe that other RFC 2355 compatible emulators may not work. Please contact the emulator product vendor directly for terms, conditions, prices and other product details related to such vendor's emulator.

For more information on the OSA-ICC single-port feature, see *System z9 and Eserver zSeries z890 and z990 Open Systems Adapter-Express Integrated Console Controller User's Guide*, SA22-7990.

OSA–ICC introduction

Your system can have one or more OSA-ICC features defined. Before you can use an OSA–ICC as a 3270 control unit, you must configure it. OSA-ICC configuration panels are accessible on your Hardware Management Console and your Support Element (SE) console. These panels allow you, the system programmer, to customize each OSA-ICC on your system.

Note: OSA-ICC's role is to provide operating systems with IPL consoles. OSA-ICC's design focus is to provide this connectivity and not to provide fast data transfers between end clients residing on the LAN and host systems. Users wishing high performance file transfer capabilities should use OSA QDIO LAN Adapters for such operations.

Dual-port network topology

The Dual-Port feature supports two physical ports per CHPID. Each port is independent and can be independently configured as an OSA-ICC. The server definition for each physical port is restricted to a unique TCP port number and subnet. These server restrictions allow isolated Local Area Networks (LAN) to be created for each physical port. The OSA-ICC dual-port function supports 120 sessions which can be randomly distributed between the two LANs. Any external network traffic will only be routed through a common default gateway defined for

both ports. An example illustrating an OSA-ICC dual-port connection is given in the network topology diagram in Figure 1.

In addition to the new port a new client connection option has also been introduced. The single client IP per session definition has been expanded to include a range of IP addresses specified by a user defined IP filter.

This document describes the new panels, tag identifiers and how to perform specific tasks using these components to configure OSA-ICC dual-port.

Figure 1 shows connectivity with OSA-ICC dual-port support where each physical port (P0, P1) is configured on a different broadcast domain (LAN). Both P0 and P1 clients communicate with OSA through the defined TCP port. The remote clients are only allowed to connect through P0 since the default gateway is associated with this port. The local clients connected to P1 are restricted to communicate only with the clients of that subnet. For more examples of different OSA-ICC dual-port network topologies, see Appendix A, "Network topology diagrams," on page 71.

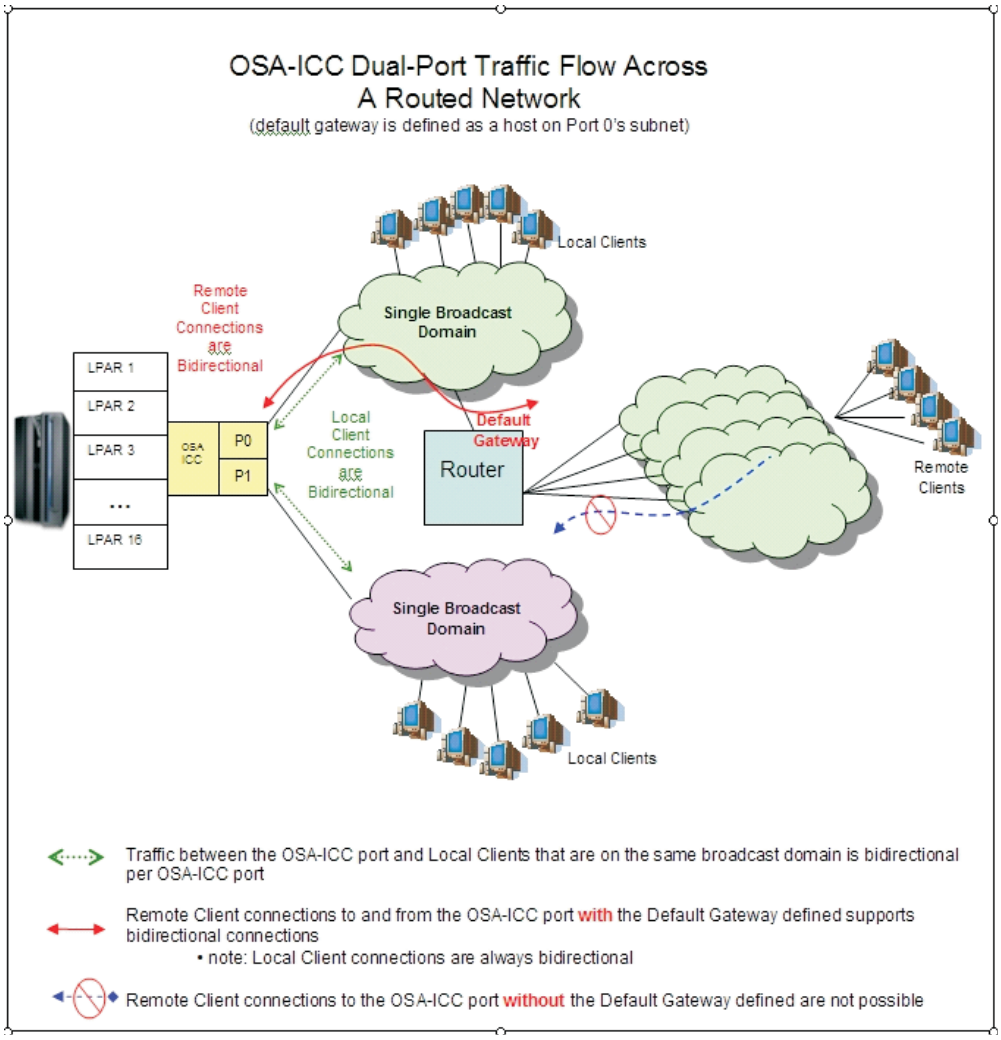

Figure 1. Network topology diagram

Planning considerations

OSA-ICC offers significant consolidation of console support. Consequently, it is strongly recommended that production environments use redundant configurations where operator consoles are defined through two different OSA-ICC LANs on two different OSA cards to prevent the loss of console control in the unlikely event of a failure. The OSA-ICC documentation and support material assumes this is the case and shows appropriate configuration information for one OSA-ICC feature.

Security concerns

Depending on how you connect your TN3270E client systems, you may or may not have security concerns. An alternative to physically local LANs is the use of one or more Virtual Private Networks (VPNs). The use of an external device or software is necessary to provide additional security for clients attaching to a host via OSA-ICC.

OSA-ICC dual-port installation and migration

Previously, OSA-ICC supported the definition of a single physical port for each CHPID. The new OSA-ICC dual-port supports two physical port definitions per CHPID. For initial installation of the OSC dual-port CHPIDs the migration process includes installing the dual-port driver, then following dual-port panel instructions to configure the server and client interface. When defining either or both physical port servers for the first time each physical port will be in the default state and there will be no sessions defined.

The migration process from single port to dual-port for a CHPID that was previously defined is automatic. After installing the dual-port driver the current single port server definition will be converted to the OSA-ICC dual-port physical port 0 definition. The second physical port will remain in its defaulted state. All dual-port specific configuration components will be automatically added to the panel and the manual configuration file to allow validation of the physical port server and client definitions. All previously defined sessions will also be transferred over as physical port 0 defined sessions.

In the event that the CHPID needs to revert to single port microcode after migrating to dual-port support, it is recommended that the configuration file associated with the CHPID is saved. If any unexpected conditions occur after applying single port microcode load, reset the CHPID to default import and apply the saved configuration file.

Chapter 2. Dual-port connection rules

The OSA-ICC dual-port configuration process includes rules for defining either or both physical ports and clients (sessions). The new rules introduced for physical port server definition allow each physical port to function independently. The server definition rules and client connection rules are described in this chapter.

z10 OSA-Express3 server definition best practices

The following server definition rules apply when defining both physical ports:

- There is a unique TCP Port number for each physical port
- There is a different subnet for each physical port host IP
- There is a single defined common gateway router with an interface on each IP Subnet; only one of the ports defines the IP Default Gateway. For more information, see Appendix A, “Network topology diagrams,” on page 71.

Client connection rules

When the client is connecting to the OSA-ICC, the client gets assigned to one of a possible 120 sessions based on what is in the client session table. If the client does not meet the criteria described below, or there are no more free sessions, that client's connection is refused. Connection rules deal with the criteria that is issued for a client’s assignment to sessions.

Connection criteria is based on two rules:

- What can be defined in the session table
- How a client is assigned to a session

There are two elements that rules deal with:

- The client's IP
- The LU name (also called group name)

The following can be defined in the session table (via panels or via source file):

- Each session has to have at least one element; for example, either LU name or an IP address.
- A session can have the client's IP and the LU name.
- A session may have only an LU name or only a client's IP.
- The same LU name cannot be specified in multiple images (CSS/IIDs). It may, however, be used multiple times within the same image.
- If a session has the LU name and IP defined, then another session cannot have that same LU name without also specifying an IP address. However, it is okay if LU is reused with the same or different IP address. If you attempt to use the LU name by itself, you will get return code 1223 or 1224, depending on what session was defined first (one with both LU name and IP address, or one with just LU name). For example:

```
session1 : CSS= 1 MIFID= 1   GROUP= "LU1"           CLIENT_IP= 10.10.10.1
session2 :  CSS= 1 MIFID= 1   GROUP= "LU1"             -
```

  These two sessions are in conflict - this would be an error.

Example 2:

```
session1 : CSS= 1 MIFID= 1   GROUP= "LU1"            CLIENT_IP= 10.10.10.1
session2 :  CSS= 1 MIFID= 1   GROUP= "LU1"            CLIENT_IP= 10.10.10.2
```

These two sessions are not in conflict.

Example 3:

```
session1 :  CSS= 1 MIFID= 1  GROUP= "LU1"            CLIENT_IP= 10.10.10.1
session2 :   CSS= 1 MIFID=1   GROUP= "LU2"               -
```

These two sessions are not in conflict - because session 2 uses a different LU.

- IP has to be unique per partition when no LU is specified.

This is how clients are assigned to a session:

- If the client has specified an LU name, then the first available session with that LU name will be considered. Furthermore, if that session entry has a client's IP address specified, the address of the incoming client must also match.
- If the client has specified an LU name, then first available session with that LU name will be considered. Furthermore, if that session entry has NO client's IP address specified, the address of the incoming client does not have to match.
- If the client has not specified an LU name, the first available session without an LU name will be considered. Furthermore, the IP address of the incoming client must match that session's client IP address.
- IP filter rule applies whenever the Client IP is defined.

Table 1. Connection rules matrix

Rule	Session configuration	Client's configuration	Effect
1	No LU name, and no IP	Not allowed	No Connection
2	Unique LU name specified	Defined LU	Connection
3	LU name specified multiple times and unique to this partition	Defined LU	Connection
		No/mismatch LU or defined in multiple CSS/image	No Connection

Table 1. Connection rules matrix (continued)

4	LU name and client IP address specified	Client specified LU name	Client IP address	
		Is valid	Client does not have an IP address	No Connection
			Client has an IP address, and there's no OSA-ICC client IP filter defined	Connection
			Client has an IP address and it matches the OSA-ICC IP filter	Connection
			The client has an IP address and it does not match the OSA-ICC IP filter	No Connection
		Is not valid	Client does not have an IP address	No Connection
			Client has an IP address, and there's no OSA-ICC client IP filter defined	No Connection
			Client has an IP address and it matches the OSA-ICC IP filter	No Connection
			The client has an IP address and it does not match the OSA-ICC IP filter	No Connection
5	Unique IP specified	IP good		Connection
		IP bad or defined in multiple CSS/images		No Connection
6	Client IP specified multiple times and unique to this partition	Defined IP		Connection
		No/mismatch IP or defined in multiple CSS/images		No Connection

Chapter 3. Defining your OSA-ICC configuration

There are four different possible Channel Path ID (CHPID) types for OSA-Express3 channels. An OSA-Express3 channel may be defined as an OSE, OSD, OSN, or an OSC CHPID. An OSA-ICC is an OSC CHPID. In order for your system to recognize an OSC CHPID, you must define the CHPID as such in your Input/Output Configuration Dataset (IOCDS) via the Hardware Configuration Definition (HCD) or the Input/Output Configuration Program (IOCP).

You must define in the IOCDS each OSA-Express3 1000Base-T port you wish to use. Each OSA-ICC function requires a unique CHPID, control unit, and device definition. These definitions are made using HCD or IOCP, which defines the OSA-Express3 feature to the I/O hardware configuration.

A TN3270E session is associated with a single device in one logical partition. You may configure a maximum of 120 sessions to be used. However, the IOCDS can contain more than 120 configurable devices.

Defining an OSC CHPID via IOCP

You can define each OSA-Express3 1000Base-T port you wish to use in the IOCDS via IOCP or HCD. The following is a sample IOCP configuration for defining an OSA-ICC channel. For instructions on defining an OSA-ICC channel via HCD, see "Steps for defining an OSC CHPID via HCD" on page 10.

```
RESOURCE PART=((CSS(0),(LP01,1),(LP02,2),(LP05,5)),                  *
              (CSS(1),(MVS1,3),(VM2,5)),                             *
              (CSS(2),(VSE,8),(LP34,4),(LP3A,A)))
CHPID PCHID=1C0,PATH=(CSS(0,1,2),80),TYPE=OSC
CNTLUNIT CUNUMBR=1000,PATH=((CSS(0),80),(CSS(1),80),(CSS(2),80)),    *
              UNIT=OSC
IODEVICE ADDRESS=(2400,96),CUNUMBR=1000,UNIT=3270,MODEL=X
```

RESOURCE PART: The RESOURCE statement defines all of the logical partitions and the logical channel subsystems (LCSSs) in the configuration. It also assigns a MIF image ID to each logical partition (for example, logical partition MVS1 has MIF ID 3 in LCSS 1).

CHPID PCHID: The CHPID statement defines a single physical port path. The OSA-Express3 port is associated with PCHID 1C0. The channel path is defined to have CHPID 80 in logical channel subsystems (LCSSs) 0, 1, and 2 and, because the PART keyword is not used, to each logical partition in the LCSSs.

CNTLUNIT: The control unit definition is assigned control unit number 1000 and has access to all 3 LCSSs. Since you can only assign a single control unit to an physical port path, be sure to include every CSS for which you want to have TN3270E sessions.

IODEVICE ADDRESS: Device numbers 2400-245F are defined and available to every logical partition in each of the LCSSs. A total of 768 devices (8 logical partitions * 96 devices) are available in the configuration but only a maximum of 120 can be configured for use.

Note: If you are using HCD to define your configuration it is important that you select control unit type OSC and device type 3270-X for OSA-ICC.

Recommendation: If you define multiple IOCDSs with different OSA configurations respectively, before Power-On-Reset, please export the OSA-ICC configuration file to a diskette. In addition, after Power-On-Reset, please import a new customized OSA-ICC configuration file from a diskette. For more information on importing and exporting your definitions, see "Import source file" on page 36 and "Export source file" on page 37.

Steps for defining an OSC CHPID via HCD

About this task

You can define each OSA-Express3 1000Base-T port you wish to use in the IOCDS via IOCP or HCD. The following is an example HCD configuration for defining an OSA-ICC channel. For instructions on defining an OSA-ICC channel via IOCP, see "Defining an OSC CHPID via IOCP" on page 9.The OSA-ICC function requires a unique CHPID, control unit, and device definition.

Note: You can only dynamically delete console devices after first removing console names with IEAVG730 or IEARELCN. For more information, see *z/OS HCD Planning*, GA22–7525 or *z/OS MVS Planning: Operations*, SA22–7601.

Channel path definition

Procedure

1. From the HCD main menu, Select option 1, and press Enter. The Define, Modify, or View Configuration Data menu is displayed.

Figure 2. Hardware configuration main menu

2. elect Option 3 "Processors", and press Enter. The Processor List is displayed.

3. Select the processor to update, and press Enter. The Actions on Selected Processors screen is displayed. The screen selection options are identified here by the action code entered, rather than the screen item number, to avoid confusion when a particular HCD menu changes.

4. On the Actions on Selected Processors screen, select S “Work with attached channel paths”, and press Enter. The Channel Subsystem List is displayed.

5. On the Channel Subsystem List, select the required CSSID, and press enter. The Actions on Selected Channel Subsystems screen is displayed.

6. On the Actions on Selected Channel Subsystems screen, select S “Work with attached channel paths”, and press Enter. The Channel Path List is displayed.

7. On the Channel Path List, press F11 to add a channel path. The Add Channel Path screen is displayed.

8. On the Channel Path List, enter the:
   - Channel path ID
   - PCHID
   - Channel path type OSC (to define the OSA-ICC function)
   - Operation mode SHR (to share this channel path among logical partitions)
   - Description

9. Complete the channel path definitions on the screen, press Enter. The Define Access List is displayed.

10. Complete the Access List for the partitions sharing the channel, and press Enter. The Candidate List Definition screen is displayed.

11. On the Candidate List Definition screen, select the partitions to include in the candidate list and press Enter, or simply press Enter if you do not want any additional partitions in the candidate list. The Channel Path List screen is displayed.

Results

Control unit definition

1. Select the CHPID just defined (CHPID 04, in our configuration), and press Enter. The Actions on selected channel paths screen is displayed.

2. On the Actions on selected channel paths screen, select S “Work with attached control units”, and press Enter. The Control Unit List is displayed.

3. On the Control Unit List, press F11 to add a control unit. The Add Control Unit screen is displayed.

4. On the Add Control Unit screen, enter the:
   - Control unit number
   - Control unit type OSC
   - Description

5. Complete the channel path definitions on the screen, and press Enter. The Select Processor / CU screen is displayed.

6. On the Select Processor / CU screen, select the processor for the control unit, and press Enter. The Actions on Selected Processors screen is displayed.

7. On the Actions on Selected Processors screen, select S for Select (connect, change), and press Enter. The Add Control Unit screen is displayed. The Add Control Unit screen shows the OSC control unit information just entered. Note the unit address is set to 00 and the number of units must be 254.

8. Confirm the control unit definitions on the screen are correct, and press Enter. The Select Processor / CU screen is displayed again.

9. Press Enter again to return to the Control Unit List screen.

Device definition

1. From the Control Unit List screen select the control unit, and press Enter. The Actions on Selected Control Units screen is displayed.

2. On the Actions on Selected Control Units screen, select S "Work with attached devices", and press Enter. The I/O Device List is displayed.

3. On the I/O Device List, press F11 to add a device. The Add Device screen is displayed.

4. On the Add Device screen, enter the:
   - Device number
   - Number of devices
   - Device type 3270-X. Device type 3270-X is the only valid device type for the OSA-ICC function. The HCD configuration process will not allow any other device type to be defined.
   - Description

5. Complete the device definitions on the screen, and press Enter. The Update Serial Number, Description and VOLSER screen is displayed, press Enter. The Device / Processor Definition screen is displayed.

6. On the Device / Processor Definition screen, select the required processor, and press Enter. The Define Device / Processor screen is displayed.

7. On the Define Device / Processor screen, you have the option of changing the starting unit address. Verify the value and press Enter. The Device / Processor Definition screen is again displayed.

8. On the Device / Processor Definition screen, press Enter. The Define Device to Operating System Configuration screen is displayed.

9. On the Define Device to Operating System Configuration screen, select the operating system to which you want to connect the devices, and press Enter. The Actions on selected Operating Systems screen is displayed.

10. On the Actions on selected Operating Systems screen, select S and press Enter. The Define Device Parameter / Features screen is displayed.

11. On the Define Device Parameter / Features screen make appropriate changes based on your environment, then press Enter. The Assign / Unassign Device to Esoteric screen will appear.

12. On the Assign / Unassign Device to Esoteric screen make appropriate changes based on your environment, then press Enter.

13. Repeat the process for each operating system as needed, then exit from the Define Device to Operating System Configuration screen, by pressing F3 or F12.

14. You should now be at the Device List panel. Press F3 multiple times to return to the main HCD screen (Hardware Configuration), for activating or processing the configuration data you just defined.

Note:

1. You can only dynamically delete console devices after first removing them with IEAVG730 or IEARELCN. For more information, see z/OS HCD Planning, GA22–7525 or z/OS MVS Planning: Operations, SA22–7601.
2. If any of the Console addresses defined are going to be used as MVS NIP consoles, then addition steps are needed:
   - Select 1 Operating system configuration
   - Select config ID with /
   - Option 6, work with consoles
   - F11 to add console addresses to the NIP CONSOLE LIST
   - Continue with the Production IODF step

You have defined the CHPID, CU, and Devices. Now complete the creation of a new production IODF and write a new IOCDS. Dynamic I/O Activation for OSC is restricted, so a POR is required to activate the configuration.

Recommendation: If you define multiple IOCDSs with different OSA configurations respectively, before Power-On-Reset, please export the OSA-ICC configuration file to a diskette. In addition, after Power-On-Reset, please import a new customized OSA-ICC configuration file from a diskette. For more information on importing and exporting your definitions, see “Import source file” on page 36 and “Export source file” on page 37.

IOCP statements

The example above converted CHPID 07 in LCSS 1 assigned to PCHID 381 from OSD to OSC, and defined control unit E300 and devices E300-E377. The following

is an example of the IOCP statements generated by HCD for the configuration of the logical partitions, both OSC CHPIDs, and the associated control unit and device definitions.

```
RESOURCE PARTITION=((CSS(0),(A0A,A),(A0B,B),(A0C,C),(A0D,D),(A*
      0E,E),(A0F,F),(A01,1),(A02,2),(A03,3),(A04,4),(A05,5),(A*
      06,6),(A07,7),(A08,8),(A09,9)),(CSS(1),(A1A,A),(A1B,B),(*
      A1C,C),(A1D,D),(A1E,E),(A1F,F),(A11,1),(A12,2),(A13,3),(*
      A14,4),(A15,5),(A16,6),(A17,7),(A18,8),(A19,9))),       *
      MAXDEV=((CSS(0),64512),(CSS(1),64512))
CHPID PATH=(CSS(0),07),SHARED,                                *
      PARTITION=((A0A,A0B,A0C,A01,A02,A03,A04,A05,A06,A07,A08,*
      A09),(=)),PCHID=380,TYPE=OSC
CHPID PATH=(CSS(1),07),SHARED,                                *
      PARTITION=((A1A,A1B,A11,A12,A13,A14,A15,A16,A17,A18,A19)*
      ,(=)),PCHID=381,TYPE=OSC
CNTLUNIT CUNUMBR=E200,PATH=((CSS(0),07)),UNIT=OSC
IODEVICE ADDRESS=(E200,120),MODEL=X,CUNUMBR=(E200),UNIT=3270
CNTLUNIT CUNUMBR=E300,PATH=((CSS(1),07)),UNIT=OSC
IODEVICE ADDRESS=(E300,120),MODEL=X,CUNUMBR=(E300),UNIT=3270
```

Refer to *Input/Output Configuration Program User's Guide for ICP IOCP*, SB10-7037 for further information about IOCP and IOCDSs.

Chapter 4. Controlling and configuring an OSA-ICC

Before you can start any TN3270E sessions, you must install an OSA-Express3 1000Base-T card and be online to the Hardware Management Console or the Support Element (SE). In order for that to happen, you must first configure your OSA-ICC by entering data in the IOCDS and then further configure your OSA-ICC via panel entry, manual entry, or a combination of both. This chapter discusses these configuration options in detail, as well as functions to control and display Information about the OSA-ICC card.

Hardware Management Console and Support Element console

You can configure your OSA-ICC from the Advance Facilities panel which is accessible from either your Hardware Management Console or your Support Element (SE) console. These two consoles are the only way you can access the OSA-ICC configuration panels. For more information on these consoles, see *Hardware Management Console Operations Guide*, SC28-6830, and *System z10 Enterprise Class Support Element Operations Guide, Version 2.10.0*, SC28-6868.

Structure of the OSA-ICC control panels

The diagram below shows the relationship of the panels which are accessed from the ***Card Specific Advanced Facilities*** panel.

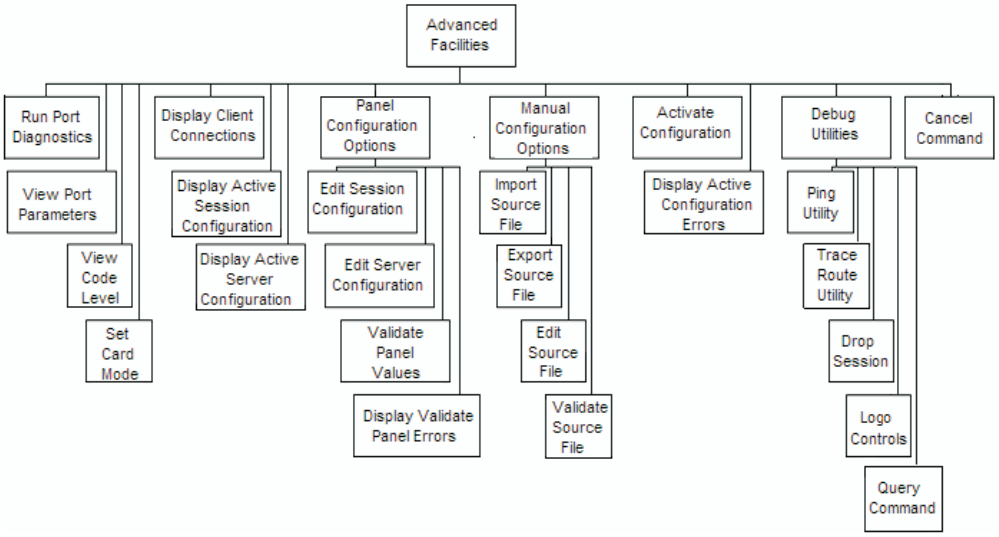

Figure 3. The structure of the configuration panels

All OSA-ICC control operations are selected from the ***Advanced Facilities*** panel as shown in Figure 7 on page 19.

The following is a brief explanation of the tasks you can perform from each of these panels:

Run port diagnostics	Allows you to run diagnostics on the physical port.

View port parameters	Allows you to view Network Interface Card statistics for the selected physical port.
Set card mode	Used to set the speed and mode of the physical port.
Display client connections	Used to view Network Interface Card statistics.
Display active session configuration	Displays the active session configuration for a given OSC.
Display active server configuration	Displays the active server configuration for a given OSC.
Panel configuration options	Allows you to edit session configurations, edit server configurations, validate panel values, and view any validate panel errors
Manual configuration options	Allows you to import a source file, export a source file, edit a source file, and validate a source file.
Activate configuration	Allows you to activate a configuration.
Display active configuration errors	Allows you to view any active configuration errors.
Debug utilities	Allows you to ping a client work station, trace the route of a packet of data to a session, and drop a session.
Cancel command	Allows you to cancel a command which is executing on an OSC.

For a complete description of the panels and the meaning of their entry fields, see "Advanced Facilities panels" on page 19.

Steps for accessing the Advanced Facilities panel

About this task

Perform the following steps to get to the Advance Facilities panel. Note that this example is using the Hardware Management Console. If you are using the SE, the initial panels to select the CHPID will be different.

Procedure

1. From the Defined CPCs Work Area, drag the selected processor to OSA Advanced Facilities.

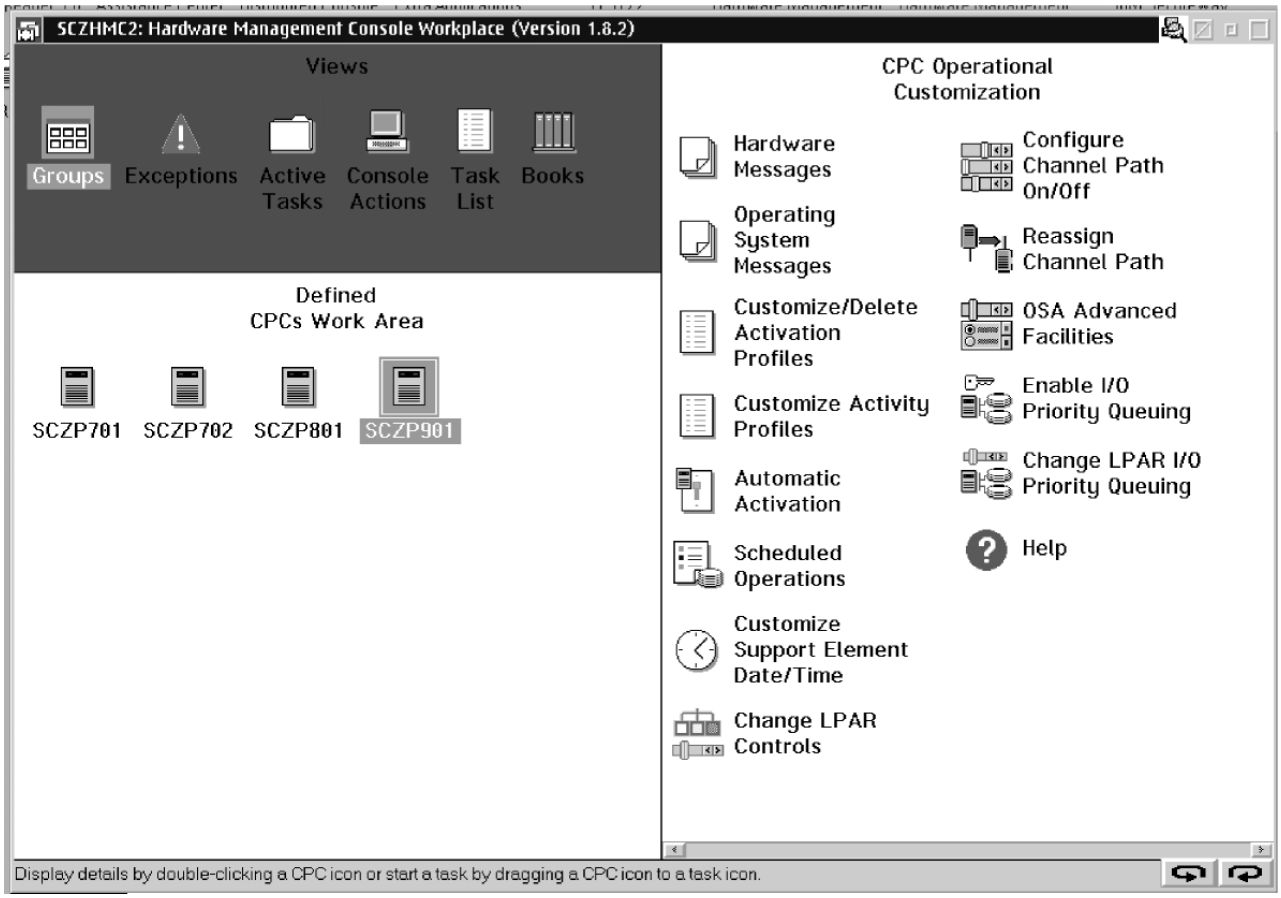

Figure 4. Hardware Management Console Workspace panel

2. The OSA Advanced Facilities panel opens. Select the PCHID you wish to configure and select OK.

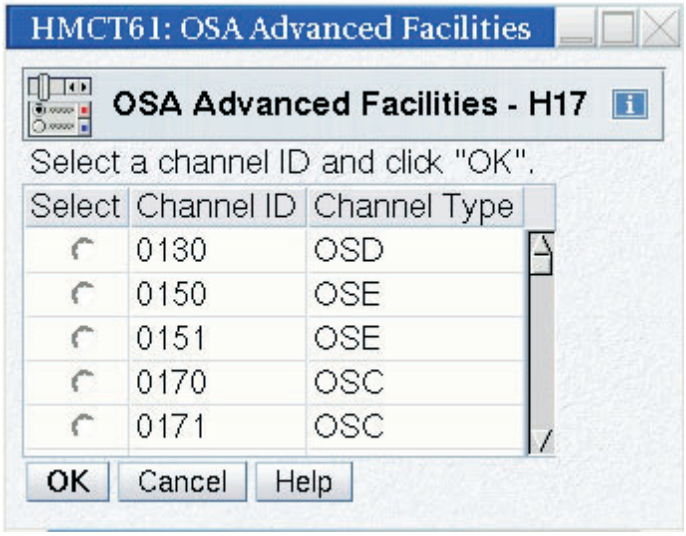

Figure 5. OSA Advanced Facilities panel

3. The ***Standard Channel Advanced Facilities*** panel is displayed. Select ***Card Specific Advanced Facilities*** and click OK.

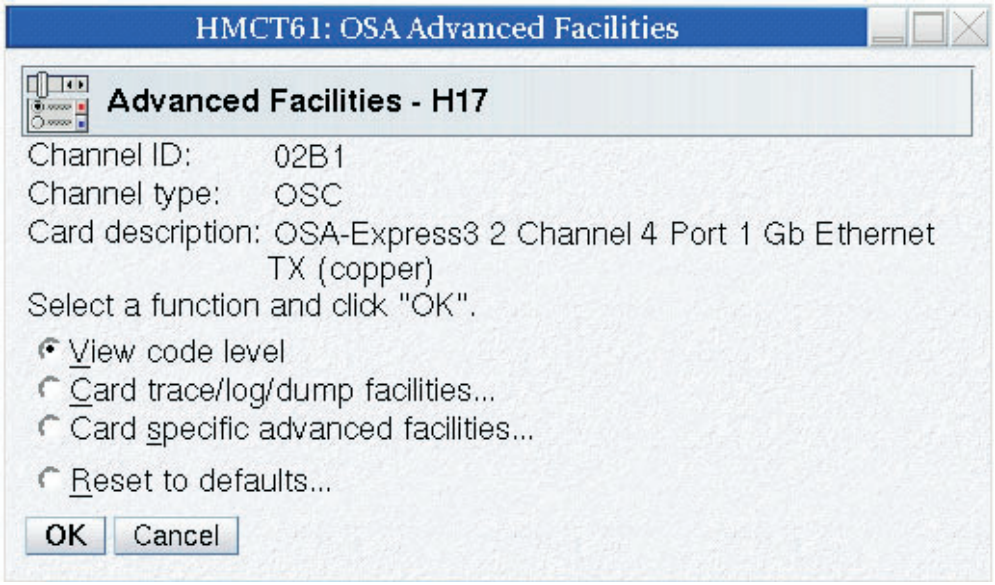

Figure 6. Standard Channel Advanced Facilities panel

Note: The View code level and Card trace/log/dump facilities... panels are not described in this document

---

Results

You should now see the ***Advanced Facilities*** panel.

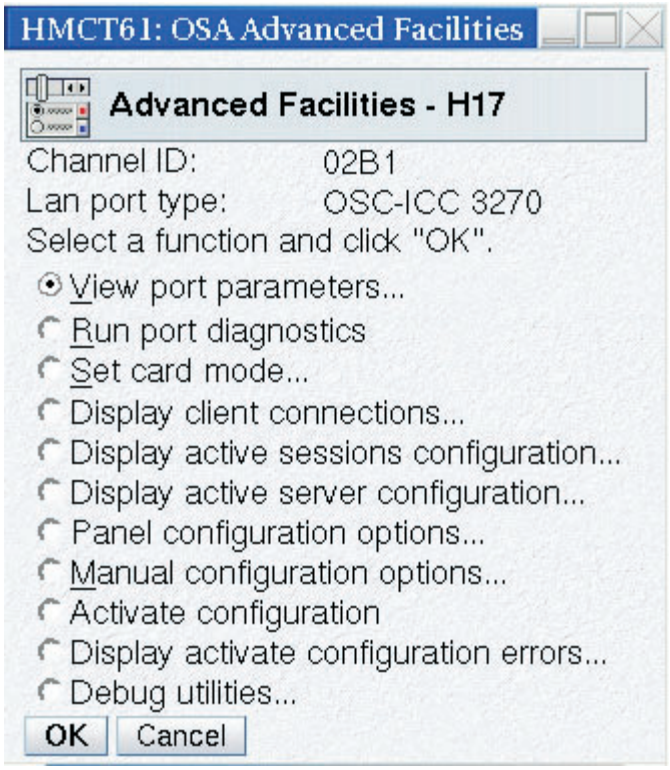

Figure 7. Card Specific Advanced Facilities panel

Advanced Facilities panels

This section describes the following OSA–ICC Advanced Facilities panels:

- View port parameters, see "View port parameters" on page 20
- Run port diagnostics, see "Run port diagnostics" on page 21
- Set card mode, see "Set card mode" on page 23
- Display client connections, see "Display client connections" on page 24
- Display active session configuration, see "Display active session configuration" on page 25
- Display active server configuration, see "Display active server configuration" on page 27
- Panel configuration option, see "Panel configuration options" on page 28
  - Edit session configuration, see "Edit session configuration" on page 28
  - Edit server configuration, see "Edit server configuration" on page 31
  - Validate panel values, see "Validate panel values" on page 33
  - Display validate panel errors, see "Display validate panel errors" on page 33
- Manual configuration options, see "Configuring via manual editing" on page 34
  - Import source file, see "Import source file" on page 36
  - Export source file, see "Export source file" on page 37
  - Edit source file, see "Edit source file" on page 39
  - Validate source file, see "Validate source file" on page 47
- Activate configuration, see "Activate configuration" on page 48

- Display activate configuration errors, see “Display activate configuration errors” on page 49
- Debug utilities, see “Debug utilities” on page 49
  - Ping utility, see “Ping Utility” on page 50
  - Trace route utility, see “Trace route utility” on page 51
  - Drop session, see “Drop session” on page 52
  - Logo Control, see “Logo Controls” on page 52
  - Query Command see “Query command” on page 53
- Cancel command, see “Cancel command” on page 53

Configuring via panel entry

Configuring your OSA-ICC results in the creation of one file containing session and server configuration information. You can create this by entering data through panel entry or by manually editing the file. Panel entry requires that you move through a series of data entry panels and enter configuration data on those panels. Panel entry is especially convenient if you want to make a small number of changes to your configuration file. Once the configuration file is created, regardless of whether it was created by panel or manual entry, either interface can be used to update the file.

View port parameters

The View port parameters panel allows you to view Network Interface Card statistics. When enabled, it gives you statistical information and setting information on your OSA-ICC. This panel is enabled after activating your server configuration. For multiple port definition, an option is provided to specify the port whose parameters will be displayed.

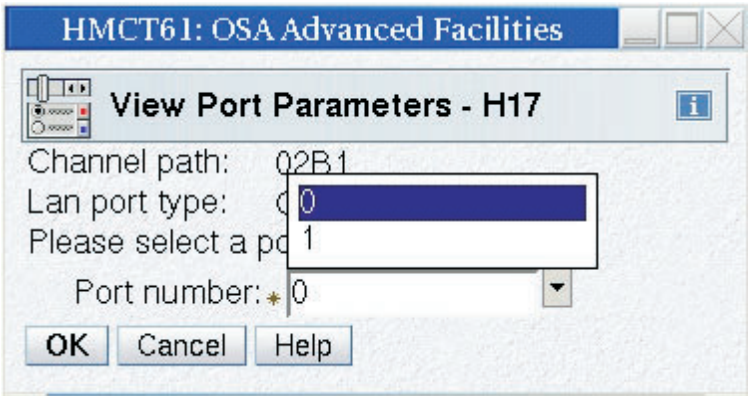

Figure 8. View port parameters panels (1 of 2)

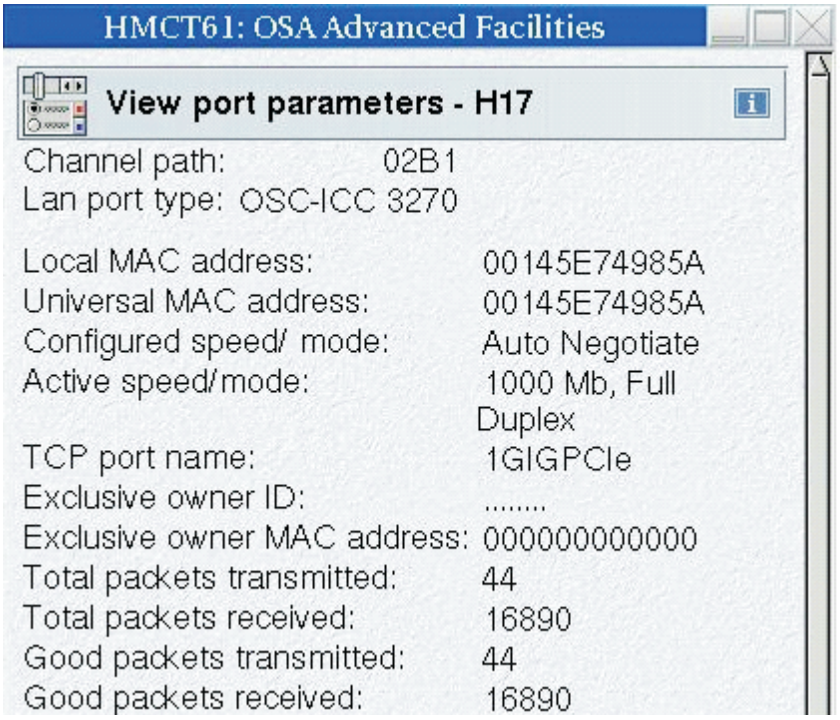

Figure 9. View port parameters panels (2 of 2)

Note: In order to see this panel, at least one port has to be configured; otherwise, the command fails with reject code A9. Appendix B, "Error codes that can be returned for an Advanced Facilities Function," on page 77 contains a list of error codes that can be returned for an Advanced Facilities Function. These errors pertain mainly to development and module communication, ensuring valid SE interface interaction; however some error codes may be encountered by the user. For panels related to validation process, Chapter 7, "Error and warning messages," on page 61 describes all the possible error codes.

Run port diagnostics

The ***Run port diagnostics*** panel is used to run diagnostics. The purpose of running these diagnostics is to check if everything is correct in the hardware. Running port diagnostics will stop all traffic on both physical ports on the CHPID.

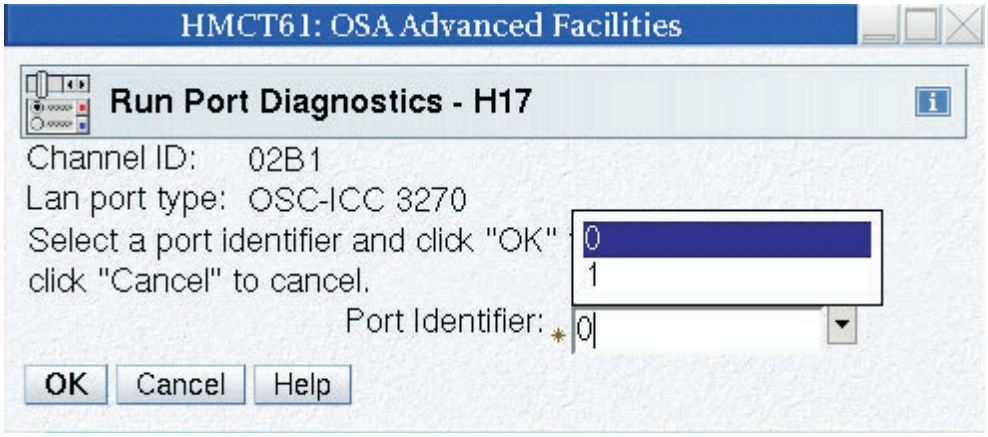

Figure 10. Run port diagnostics panel

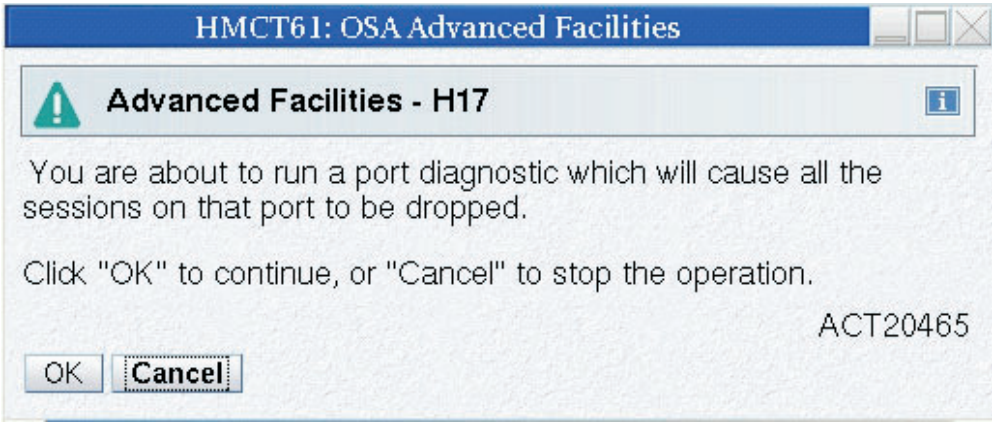

Figure 11. Run port diagnostics warning panel

Physical port identifier: Identifies the port you want to run diagnostics on. Since there is only one port in OSA-ICC, the entry field default is 0. However, the desired port can be selected by using the pull down menu.

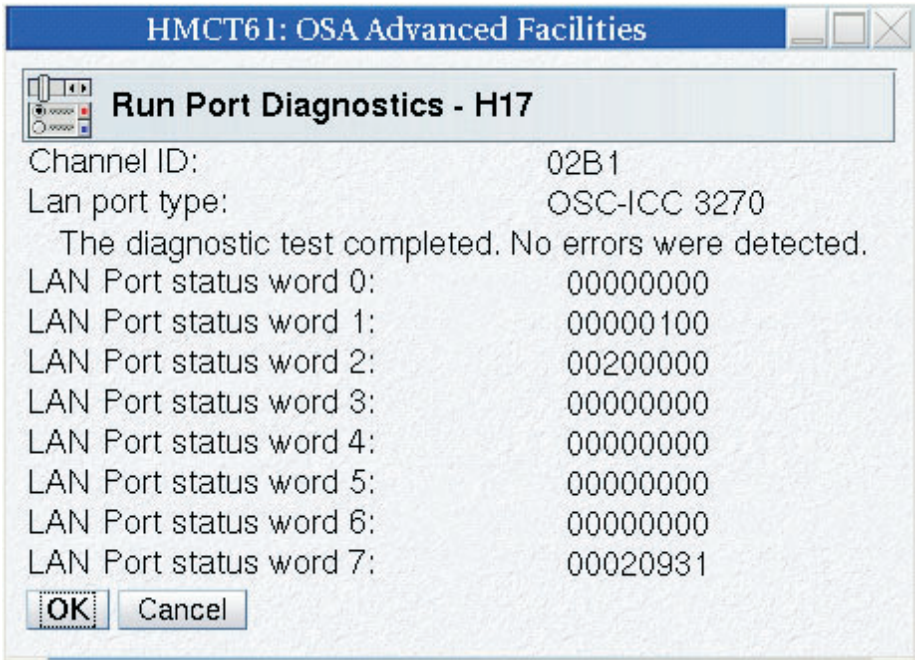

Figure 12. Run port diagnostics panel

Set card mode

The ***Set card mode*** panel is used to set the speed and mode of the OSA-ICC.

Note: This panel does not show the way the card is currently set. It is not a display card mode panel. This panel shows options to set the card. See "View port parameters" on page 20 to see how the card is set.

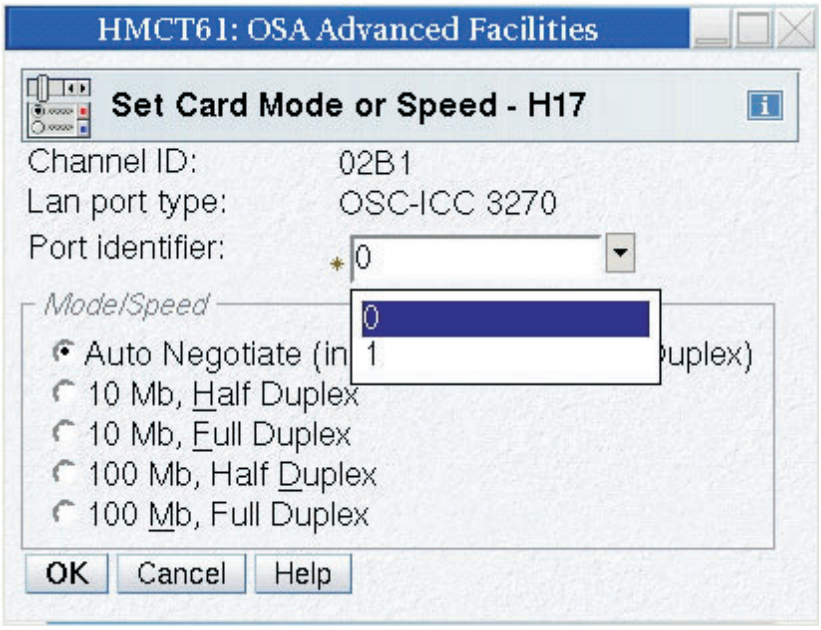

Figure 13. Set card mode panel

Physical port identifier: Since there are multiple ports, a selection is made to specify which port speed to set. By default this field is set to zero.

Speed/Mode: The default is Auto Negotiate. If auto-negotiate fails, the default is 100 Mb, half duplex. The speed/mode is changed dynamically, but it is recommended that you do not make this change while sessions are active and connected.

Display client connections

The ***Display client connections*** you to view currently connected clients. This information is queried at the time you open this panel. To refresh the information, exit the panel and reopen it.

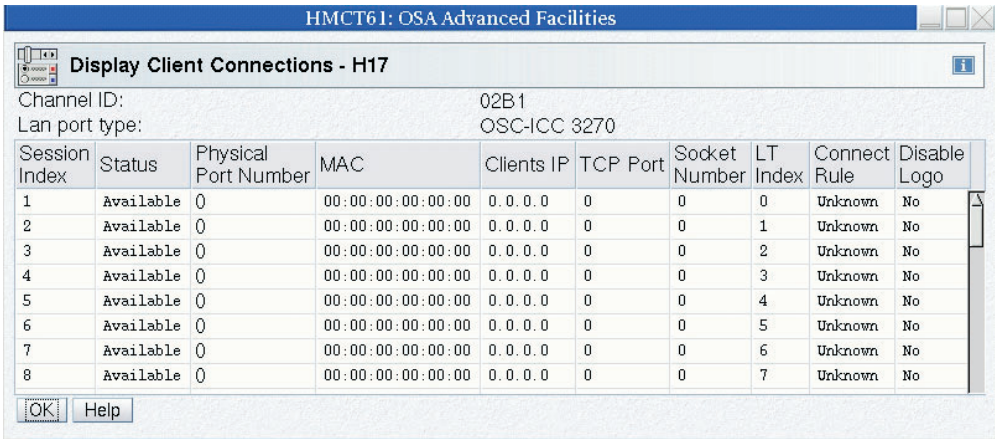

Figure 14. Display client connections panel

Session Index specifies the session number. The valid range is from 1–120.

Status specifies whether the session is not configured, available, connected, active, or definition error:

- Not configured: the session has not yet been configured.
- Available: the session has been configured and the client can connect to it.
- Connected: the session has been configured and the client is connected to it.
- DHD pending: the client has been disconnected. However, since DHD was enabled, OSA-ICC has not notified the host operating system yet.
- Definition error: the session is not a valid session and the client cannot connect. The session CSS, MIFID, or Device Number does not exist or was dynamically deleted during dynamic I/O.

Physical Port Identifier displays which server port the client is connecting through.

MAC specifies the address of the client that is being connected if the client is on the local end. Otherwise, the MAC address of the router is displayed.

Client's IP specifies the IP address of the attached client.

Port specifies the port number of server which the client will connect through

Socket Numbers specifies the Local TCP socket number that uniquely defines the connection. This parameter is only useful to the OSA-ICC PE.

LT Index specifies the index in the LT table. A valid range is from 1–120. This parameter is only useful to the OSA-ICC PE.

Connect rule can be IP only, LU only, IP & LU, unknown. For more information on connection rules, see Chapter 2, “Dual-port connection rules,” on page 5.

LOGO this feature has two values ENABLE/DISABLE. When enabled the three line logo appears on client session, if disabled this three line logo will not appear. For more information on the three line logo display, see Section 4.

Display active session configuration

The ***Display active session configuration*** panel is used to display the active session configuration for a given OSC. This includes a list of the sessions that are configured for the OSC and configuration information about each session.

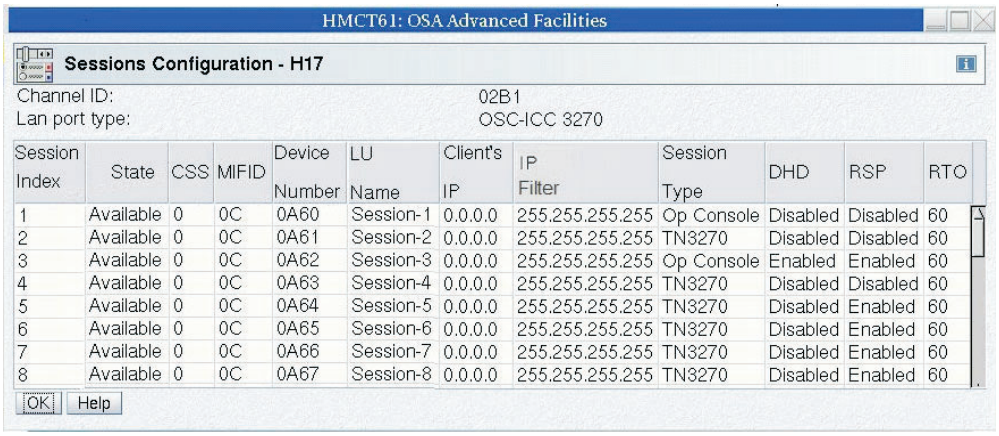

Figure 15. Display active session configuration panel

Session Index specifies the session number.

State specifies whether the session is not configured, available, or has a definition error:

- Not configured: the session has not yet been configured.
- Available: the session has been configured and the client can connect to it.
- Definition error: the session is not a valid session and the client cannot connect. The session CSS, MIFID, or Device Number does not exist or was dynamically deleted during dynamic I/O.

CSS specifies the logical channel subsystem ID. The valid range for CSS is 0–3.

MIFID is the logical partition MIF image ID. A valid range for the Image Id is 1–F.

Device Number is a number assigned for each device that was defined in the IOCDS.

LU Name defines a group or pool of devices that identifies what session you are going to connect to.

Client's IP (optional) specifies the IP address that client will use to connect to the session. The client's IP address can remain 0.0.0.0 or empty in order to allow any client to connect to a specific session. If a non-zero IP is specified, any client with a non-matching IP is rejected.

IP Filter gives a range of client IP addresses that are allowed to connect through a given physical port. This IP filter is only applicable when the client's IP address is specified.

Session Type can be console, operating system console, or printer.

DHD (Defer Host Disconnect) indicates the amount of time to wait (in seconds) until OSA-ICC tells the host that the client session has disconnected.

RSP (Response Mode) indicates if response mode is enabled or disabled. If enabled, the host waits for the client to send an acknowledgement on the Telnet level for every packet that is transmitted. This enables the user to check for bad LANs, poor performance, or other issues.

RTO (Response Time Out): specifies how long to wait (in seconds) for a response from the client before performing a client disconnect. The default RTO is 60. The valid range for RTO is 1-300.

Note:

1. The phrase Response Time Out and Read Time Out are synonymous for OSA-ICC
2. If no RTO is specified, the Missing Interrupt Handler (MIH) should be disabled.
3. If an RTO value is specified, MIH should be set to at least 50% greater than the RTO value. MIH is set via the operating system.

Display active server configuration

The ***Display active server configuration*** panel is used to display the active TCP/IP connection configuration information about the physical port.

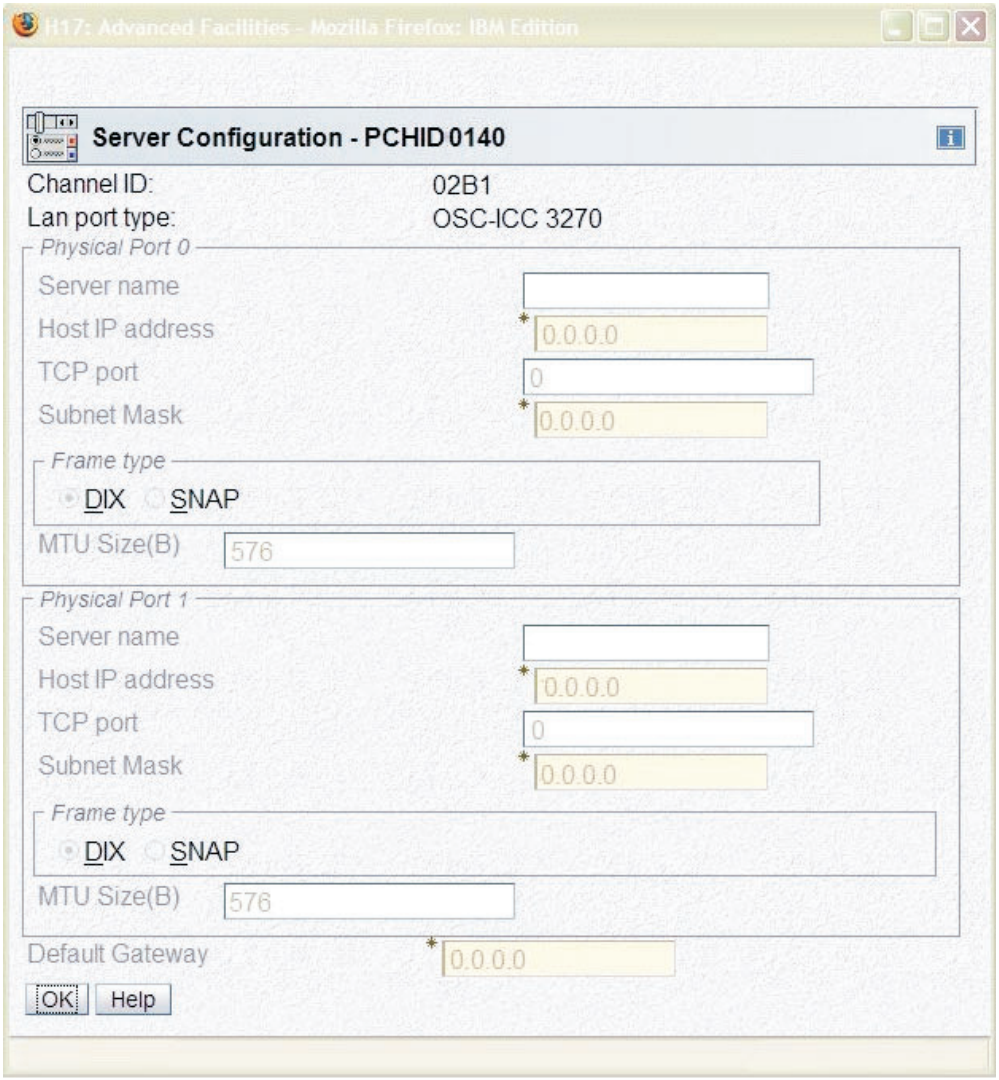

Figure 16. Display active server configuration panel

Server Name specifies the name of the server to which a client is connected.

Host IP Address specifies your IP address.

TCP Port specifies the port that the server will use to connect with the client.

Default Gateway specifies IP address gateway to any machines out of network.

Subnet Mask specifies a mask used to determine the subnet to which an IP address belongs.

Frame type specifies the Ethernet standards that you want the network to follow. Every host in a network must have the same frame type. It is **strongly recommended** that you use DIX as your frame type. SNAP refers to IEEE 802.2 framing, but most traffic on Ethernet is usually carried on DIX (802.3) frames. Please contact your network administrator to see what you are using.

MTU Size(B) specifies the maximum size to be transferred in one frame. A valid range is from 64–1492. A user would use an MTU size of less than 1492 when the routing equipment does not support anything above 576.

Panel configuration options

The ***Panel configuration options*** panel is the high level selection panel for the configuration options that are used for editing a session or server configuration, validating panel values, and/or viewing validate panel values errors. To choose a panel configuration option, select a utility option and click OK.

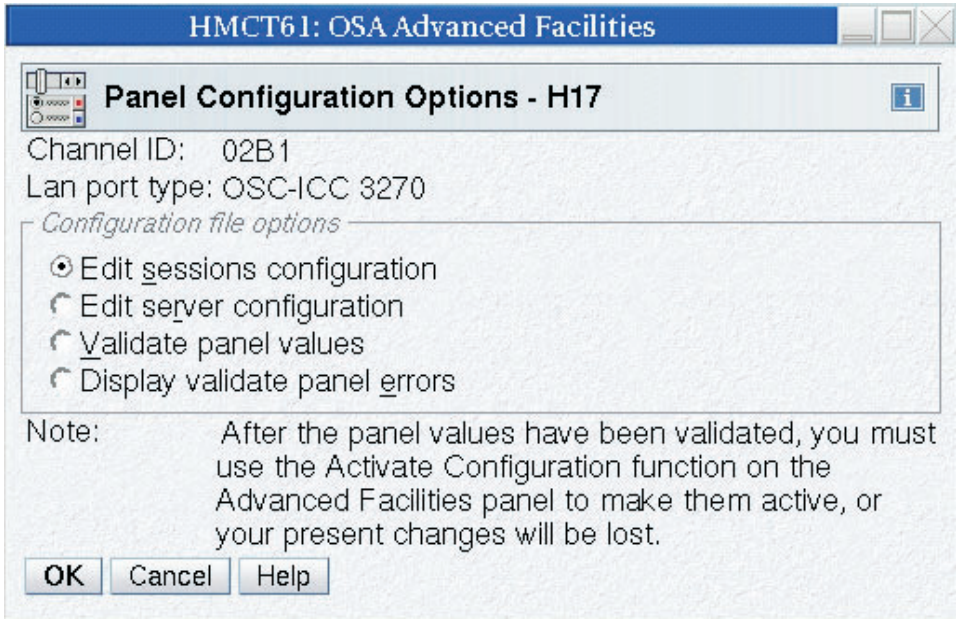

Figure 17. Panel configuration options panel

Edit session configuration

The ***Edit session configuration*** panel is used to edit the session configuration for a given OSC. This includes a list of the sessions that are configured for the OSC and configuration information about each session. The display is the same as the ***Display active session configuration*** panel except the fields may be edited.

Note: In order to make your edited session the active configuration, you must validate then activate it. For more information about validating, and activating see

"Validate panel values" on page 33 and "Activate configuration" on page 48. In addition, you may want to export your source file as a backup. For more information on exporting, see "Export source file" on page 37.

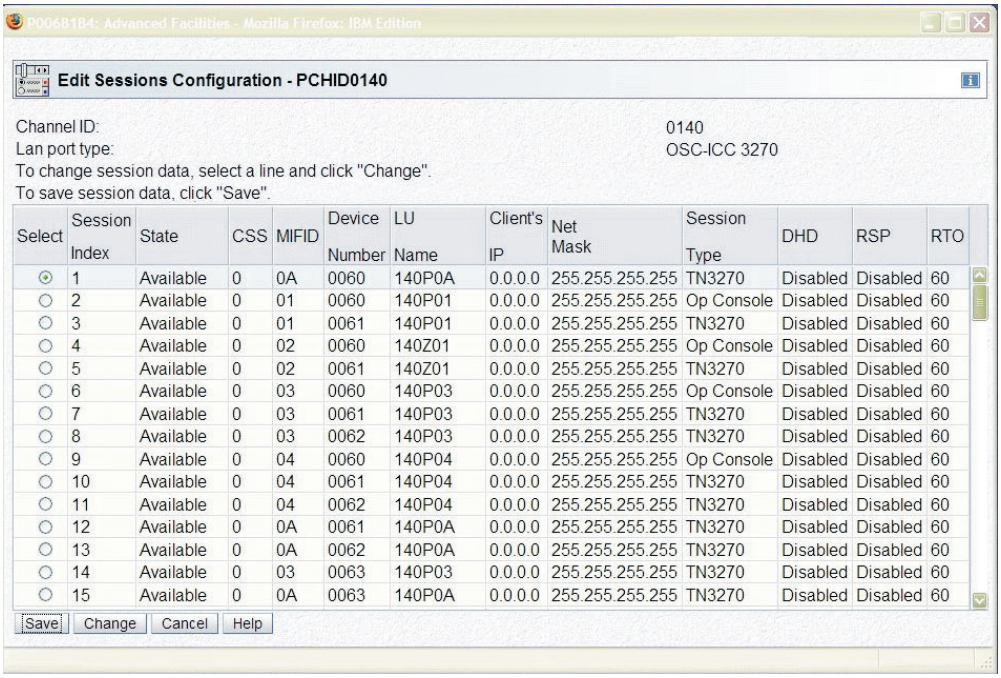

Figure 18. Edit session configuration panel

Index specifies the session number.

State specifies whether the session is not configured, available, or has a definition error:

- Not configured: the session has not yet been configured.
- Available: the session has been configured and the client can connect to it.
- Definition error: the session is not a valid session and the client cannot connect. The session CSS, MIFID, or Device Number does not exist or was dynamically deleted during dynamic I/O.

CSS specifies the logical channel subsystem (LCSS) ID number. A valid range for CSS is 0–3.

MIFID is the logical partition MIF image ID. It specifies the logical partition within the LCSS with which the device will communicate. A valid range for the Image Id is 1–F.

Device Number is a number assigned for each device. A valid range for the device number is 0-65535.

LU Name defines a group pool of devices. Identifies what session you are going to connect to. This field is not case-sensitive.

Client's IP (optional) specifies the IP address that client will use to connect to the session. The client's IP address can remain 0.0.0.0 or empty in order to allow any client to connect to a specific session.

IP Filter (optional) defines a range of IP addresses that can connect to the session. Clients IP addresses that match the range of the IP filter will be allowed to connect. Likewise clients with IP addresses outside the range of the IP_FILTER requesting to connect will be refused a connection. The IP filter is applied to the Client's IP in the same manner in which a network subnet mask is applied to the host IP. This field is assigned the value 255.255.255.255 by default.

Session Type can be TN3270, operating system console, or printer. The default is the operating system console.

DHD (Defer Host Disconnect): indicates the amount of time to wait (in seconds) until OSA-ICC tells the host that the client session has disconnected. For example, if you wanted to turn your PC off without the host knowing you left, you would click on the radio button for "enable with no timeout for deferment." This option specifies that the host will never be informed that you have logged off. A valid range for DHD is 1-86400 (24 hours in seconds).

RSP (Response Mode) indicates whether response mode is enabled or disabled. If enabled, the host waits for the client to send an acknowledgement on the Telnet level for every read, write, or packet it receives. This enables the user to check for bad LANs, poor performance, or other issues.

RTO (Response Time Out) specifies how long to wait (in seconds) for a response from the client before performing a client disconnect. The default RTO is 60. The valid range for RTO is 1-300.

Note:

1. The phrase Response Time Out and Read Time Out are synonymous for OSA-ICC
2. If no RTO is specified, Missing Interrupt Handler (MIH) should be disabled. If an RTO value is specified, MIH should be set to at least 50% greater than the RTO value. MIH is set via the operating system.

To edit a field:

1. Highlight the entry you want to edit
2. Double click the change button at the button of the screen
3. Make any desired changes. Be sure to scroll down to view all the fields that you can edit. For a description of the fields, see the field descriptions above.
4. 4. Click OK to save the updated session information or the information will be lost.
5. Validate and activate your changes. For more information on validating and activating see, "Validate panel values" on page 33, and "Activate configuration" on page 48. In addition, you may want to export your configuration as backup. For more information on exporting, see "Export source file" on page 37.

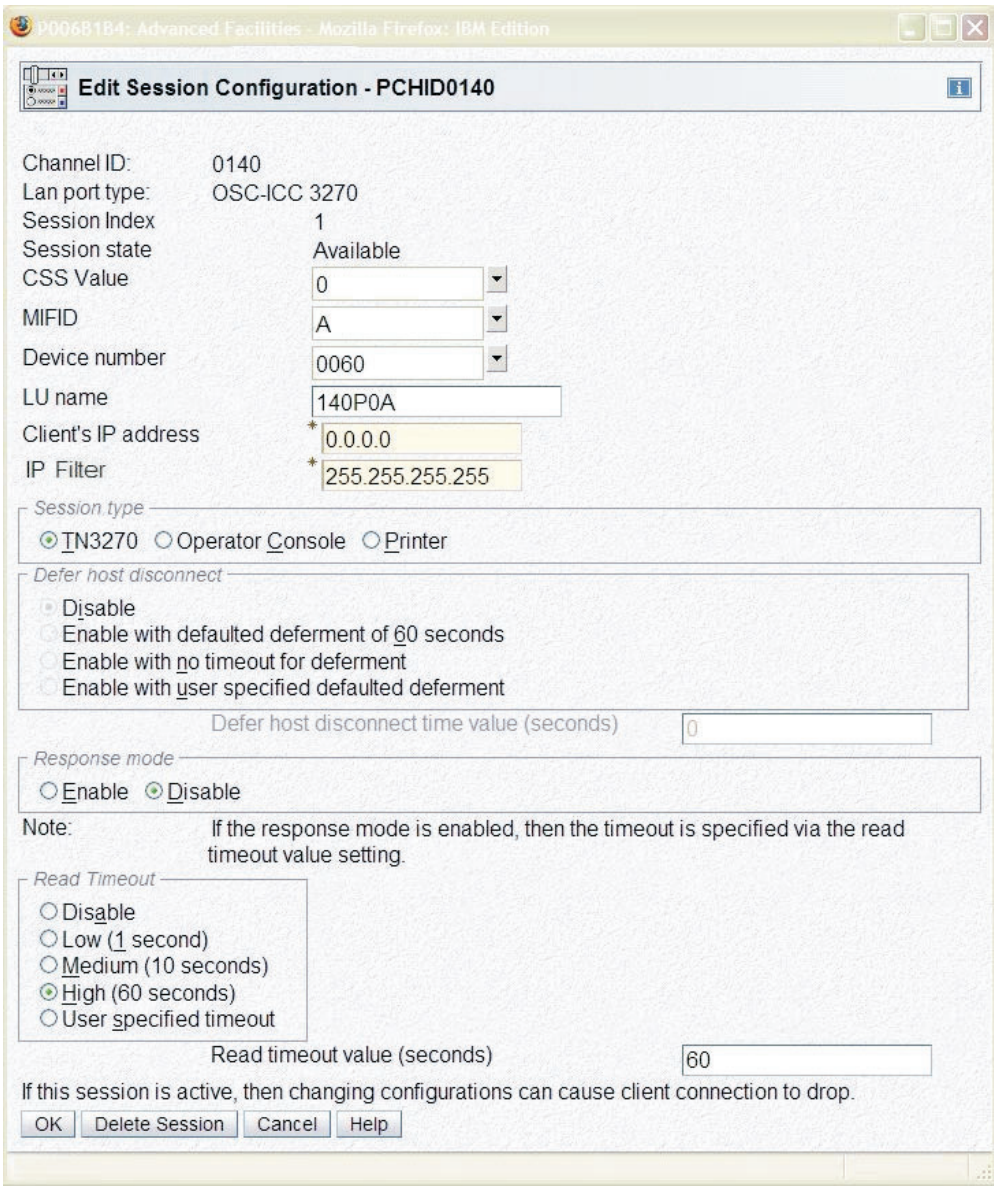

Figure 19. Edit session configuration panel

Edit server configuration

The ***Edit server configuration*** panel is used to edit the server configuration for a given OSC. For this panel the option is given to configure a single port or both. If both ports are configured and the user wishes to disable a given port the values for Host IP address, TCP port and Subnet Mask must be set to the default state (zero). At least one port must be defined at a given time in order for the server to be configured. An example of disabled Port 1 and enabled Port 0 is shown in Figure 20 on page 32.

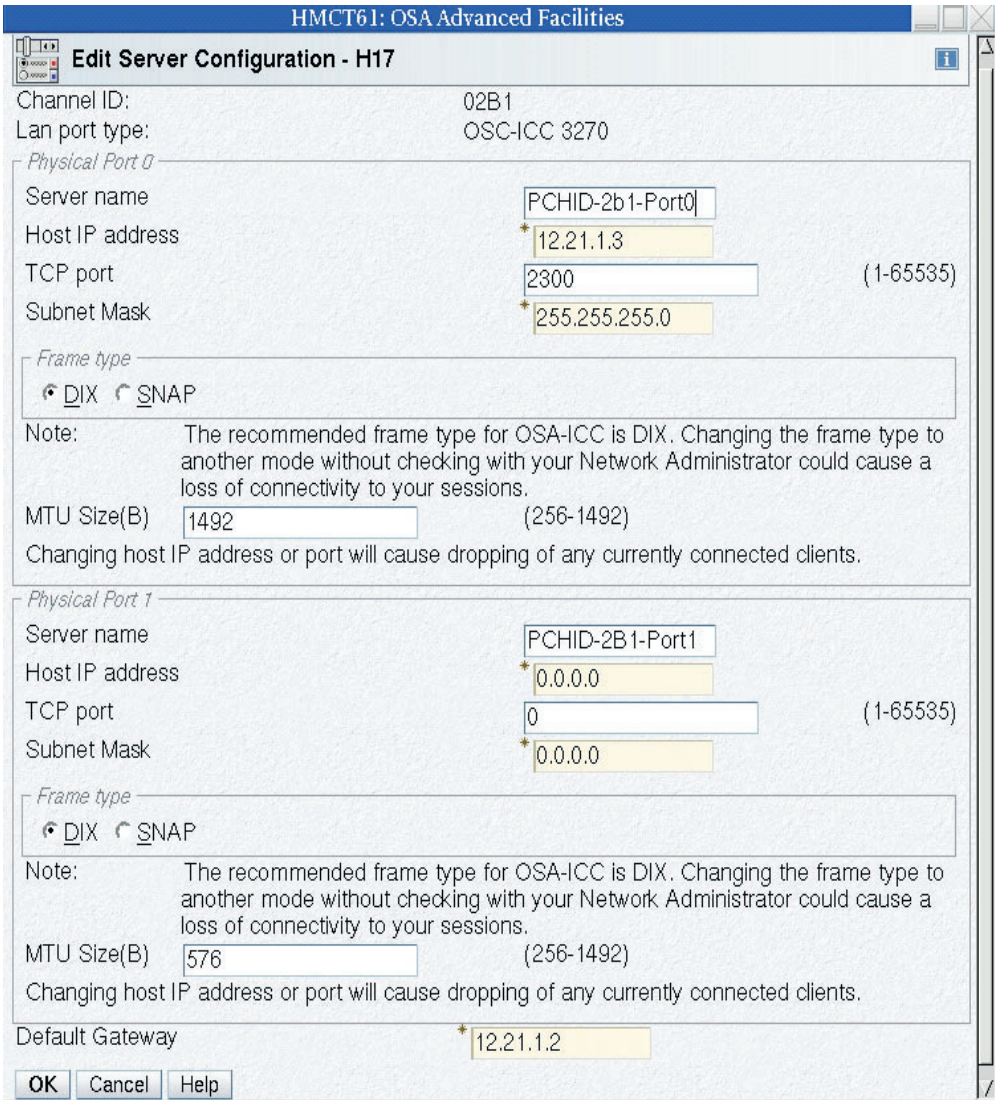

Figure 20. Edit server configuration panel

The *Edit server configuration* panel requires the following input:

Server name Used for display only.

Host IP Address specifies your IP address.

TCP Port Port that the server will use to connect with the client. A valid range is 1–65536.

Default Gateway specifies the IP address, in dotted decimal format, of the default gateway (router) that will forward all traffic that is not destined to a local host residing on a network that one of the OSA-ICC ports is physically connected to. Only one Default Gateway can be specified for either single port, or multi-port deployments.

The default gateway must not be blank; it must contain a dotted decimal IP address, otherwise a panel error will be flagged. Note that 0.0.0.0 is allowed as a valid input.

Note that the IP address you specify is not checked as part of the configuration validation operation to determine if the respective router is reachable via either OSA-ICC port. Therefore, you must ensure that the host at the respective address is not only reachable through one of the OSA-ICC ports, but that it will also satisfy your IP routing requirements.

Subnet Mask determines what subnet an IP address belongs to.

Frame type specifies the Ethernet standards that you want the network to follow. Every host in a network must have the same frame type. It is **strongly recommended** that you use DIX as your frame type. SNAP refers to IEEE 802.3 framing, but most traffic on Ethernet is usually carried on DIX frames. Please contact your network administrator to see what you are using.

MTU Size(B) specifies the maximum size to be transferred in one frame. A valid range is from 256–1492. The default is 1492. Speak to your network administrator to see if you need the MTU size to be different from the default.

Validate panel values

The ***Validate panel values*** panel is used to validate any values entered in the configuration panels.

Note:

1. In order to make your validated session the active configuration, you must activate it. For more information about activating see "Activate configuration" on page 48. In addition, you may want to export your source file as a backup. For more information on exporting, see "Export source file" on page 37.
2. 2. For a list of errors and warnings that you might receive after validating, see Chapter 7, "Error and warning messages," on page 61.

If you receive errors during your validation, you must fix them before you can activate the configuration. If you receive warnings during your validation, you may still activate your configuration. However, it is suggested that you address these warnings and re-validate before you activate your configuration.

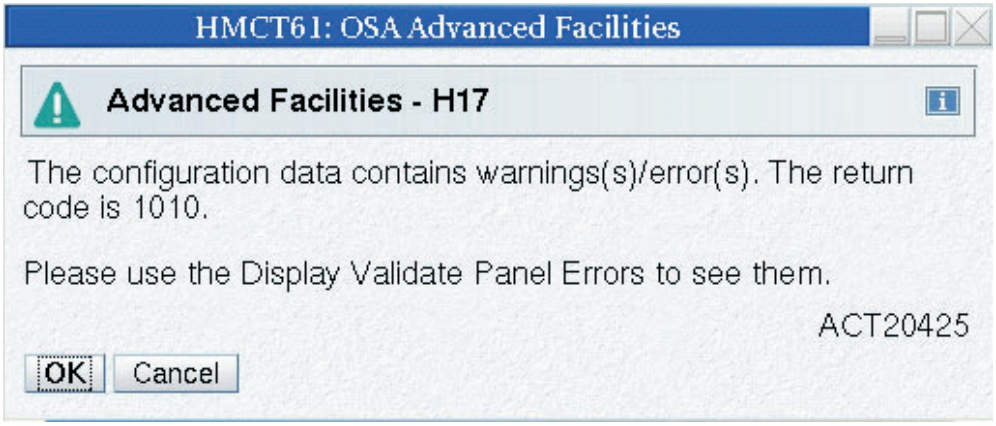

Figure 21. Validate panel values panel

Display validate panel errors

The ***Display validate panel errors*** panel is used to view any errors you might have received while validating. For a list of errors and warnings that you might receive,

see Chapter 7, “Error and warning messages,” on page 61.

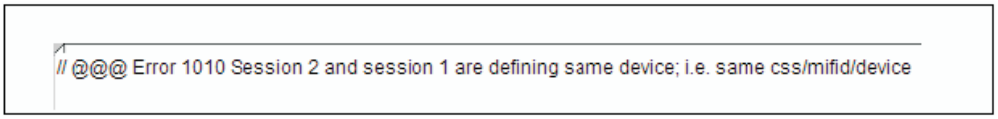

Figure 22. Display validate panel errors panel

Configuring via manual editing

Configuring your OSA-ICC results in the creation of a session configuration file. You can create this file by entering data via panel entry or by manually editing the file. Panel entry requires that you move through a series of data entry panel and enter configuration data on those panels. Your other option is to edit your configuration manually using your favorite workstation editor. Manual editing is much faster for multiple data entries because of the powerful editing capabilities of most workstation editors.

You can edit the configuration file on your Hardware Management Console or SE console or you can export the configuration file to a diskette, edit it on the workstation of your choice, and import back to the SE. You can also edit the configuration file directly on the SE console by selecting the ***Edit source file*** panel under the ***Manual configurations options*** panel. The configuration file is named IQZC*xxxx*.trm (*xxxx* is the PCHID number where the 1000Base-T port is located) and is referred to as the 'source' file on the related panels.

Before you begin: In order to perform a manual operation on your configuration file you must use the panels on the SE to get to the ***OSC manual configuration*** panel. For details about how to get to the card specific ***Advanced facilities*** panel, see “Steps for accessing the Advanced Facilities panel” on page 16.

1. From the ***Advanced facilities*** panel select ***OSC manual configuration.***You will see the ***OSC manual configuration*** panel.

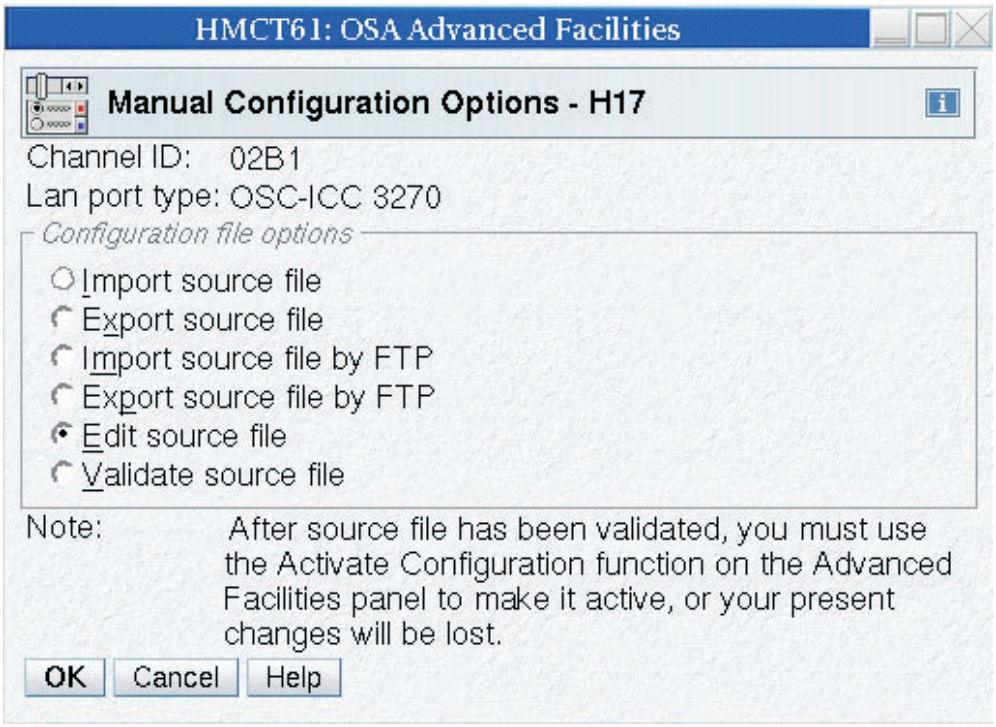

Figure 23. OSC manual configuration panel

2. Export source file (optional). For more information about exporting source files, see "Export source file" on page 37.
3. Edit source file. For more information about editing source files, see "Edit source file" on page 39.
4. Import source file (optional). For more information about importing source files, see "Import source file" on page 36.
5. Validate source file. For more information about validating source files, see "Validate source file" on page 47.
6. Activate configuration. For more information about activating a configuration, see "Activate configuration" on page 48.

Manual configurations options

The ***Manual configurations options*** panel is the high level selection panel for the manual configuration options that are used for importing a source file, exporting a source file, editing a source file, and validating a source file. Manual configuration is the most efficient way to create a configuration file because it allows you to create and modify a configuration file with the editor of your choice. Many editors allow you to copy and paste sections of the file and to find and replace data items quickly and easily.

The dual-port configuration file has new components that allow the validation of the defined physical ports. When configuring through the manual option, these components will, by default, appear in the file. If only one physical port will be defined, the default data of the other physical port must be removed in order for the validation process to be successful.

To choose a manual configuration option, select a utility option and click OK.

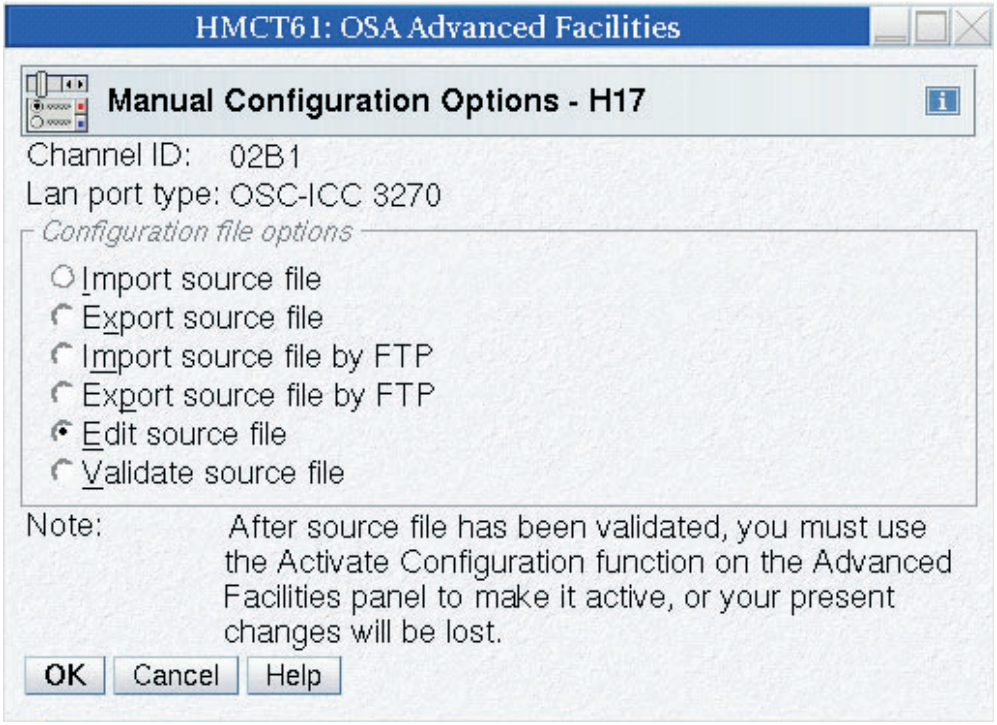

Figure 24. Manual configuration panel

Import source file

Any exported configuration file that has been modified must be imported before the changes can be applied. Here are the steps for importing a session configuration file from a USB flash drive or other supported device.

Note: In order to make the imported source file the active configuration, you must edit the source file (optional), validate the source file and then activate it. For more information about editing, validating, and activating source files see, "Edit source file" on page 39, "Validate source file" on page 47 and "Activate configuration" on page 48. In additon, you may want to export your source file as a backup. For more information on exporting, see "Export source file" on page 37.

Steps for importing a configuration file: **Before you begin**: You must be aware of the naming requirements for a configuration file. These requirements are that the filename has a maximum of eight characters.

1. Insert USB flash drive or other supported device containing the source file into your USB flash drive or other supported device. If you are working from the SE, your import will be from the SE. If you are working from the Hardware Management Console, the import will be from the Hardware Management Console. If your Hardware Management Console is in single object operation, you must insert the USB flash drive or other supported device in the SE
2. From the ***Manual configuration options*** panel select ***Import source file*** . The ***Import source file*** panel appears with a list of all the files on the disk.

   For example:

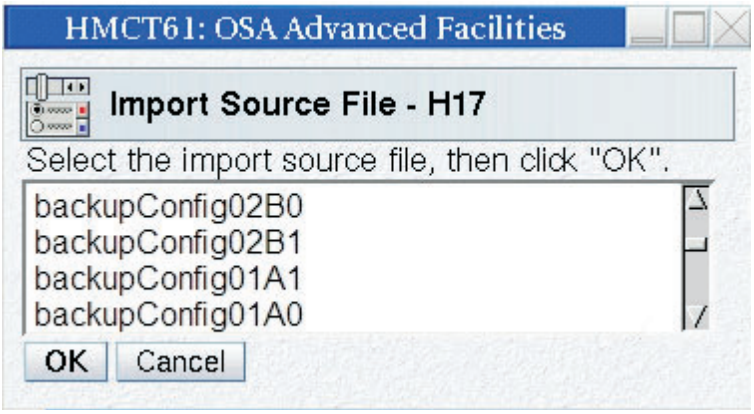

Figure 25. Import source file panel

3. Highlight the file you would like to import and click *OK*. The file you specified will be imported.

   Warning: Although you can import any file listed, trying to validate and activate a file that is not a configuration file will fail.

4. 4. Edit (optional), validate your imported source file, and activate the configuration.

For an example of a source file, see "Example of a correct configuration file" on page 40.

Export source file

The ***Export source file*** panel is used to export a session configuration file to a USB flash drive or other supported device so you can edit the configuration file with your editor. You can also use this panel to export your configuration options as a backup. Here are the steps for exporting the session configuration file to a USB flash drive or other supported device.

Steps for exporting a configuration file: **Before you begin**: You must be aware of the naming requirements for a configuration file. These requirements are that the filename has a maximum of eight characters.

1. Insert USB flash drive or other supported device containing the source file into your USB flash drive or other supported device. If you are working from the SE, your import will be from the SE. If you are working from the Hardware Management Console, the import will be from the Hardware Management Console. If your Hardware Management Console is in single object operation, you must insert the USB flash drive or other supported device in the SE.
2. From the ***Manual configuration options*** panel select ***Export source file***. The ***Export source file*** will appear.

   For example:

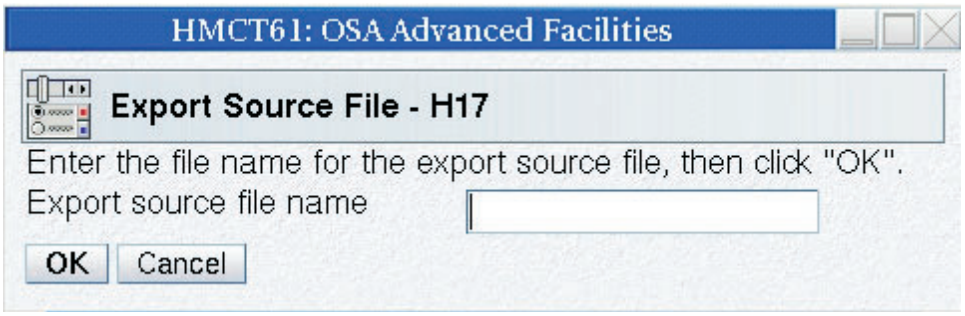

Figure 26. Export source file panel

3. Type in the name to be given to the exported configuration file in the Export source file name field and click OK. The panel is going to export the configuration file for the PCHID selected.

Import source file via FTP

If you exported a configuration file for editing you must import it in order to use it. Here are the steps for importing a session configuration file via FTP.

Note: In order to make the imported source file the active configuration, you must edit the source file (optional), validate the source file and then activate it. For more information about editing, validating, and activating source files see "Edit source file" on page 39, "Validate source file" on page 47 and "Activate configuration" on page 48. In addition, if you update the file you may want to export your source file as a backup. For more information on exporting, see "Export source file via FTP" on page 39.

Steps for importing a configuration file via FTP: **Before you begin**: You must be aware of the naming requirements for a configuration file. These requirements are that the filename has a maximum of eight characters.

1. From the ***Manual configuration options*** panel select ***Import source file via FTP***. The ***Import source file via FTP*** will appear.

   For example:

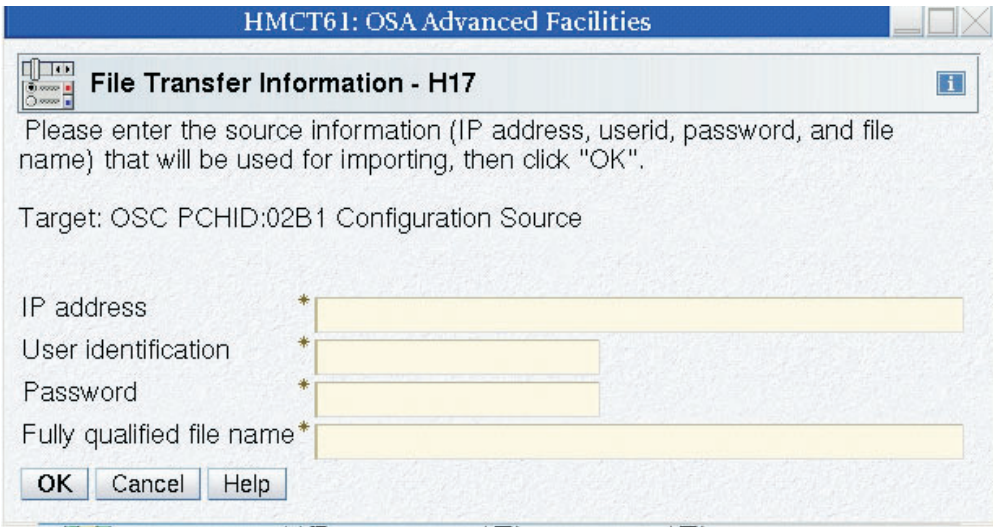

Figure 27. Import source file via FTP panel

2. Enter the IP address, user identification, password, and fully qualified file name and click OK. The file you specified will be imported.

   Warning: Although you can import any file listed, trying to validate and activate a file that is not a configuration file will fail.

3. Edit (optional), validate your imported source file, and activate the configuration. For an example of a source file, see "Example of a correct configuration file" on page 40.

Export source file via FTP

The **Export source file via FTP** panel is used to export a session configuration file via FTP so you can edit the configuration file with your editor. You can also use this panel to export your configuration options as a backup. Here are the steps for exporting the session configuration file via FTP and editing it on your workstation of choice.

Steps for exporting a configuration file via FTP: **Before you begin**: You must be aware of the naming requirements for a configuration file. These requirements are that the filename has a maximum of eight characters.

1. From the ***Manual configuration options*** panel select ***Export source file via FTP***. The ***Export source file via FTP*** will appear.

   For example:

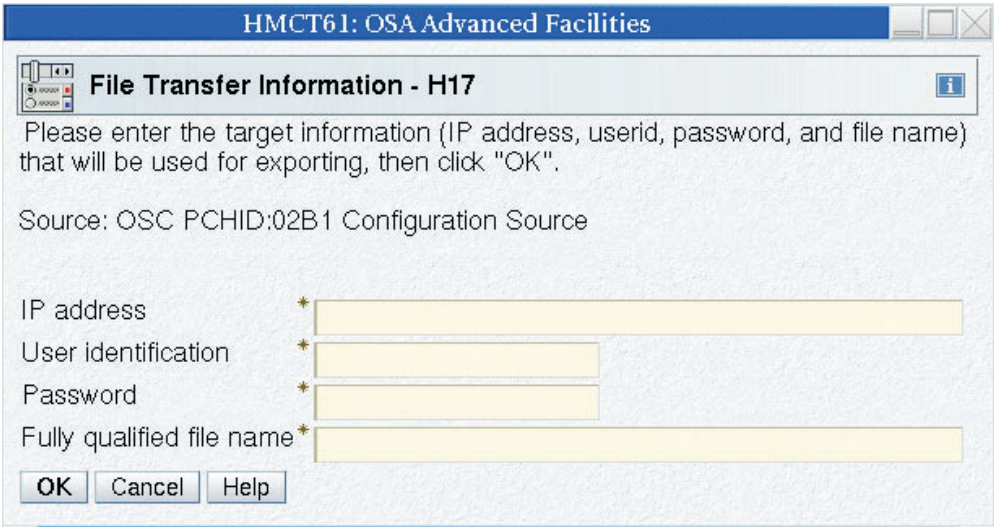

Figure 28. Export source file via FTP panel

2. Type in the IP address, user identification, password, and fully qualified file name to be given to the exported configuration file and click OK. The panel is going to export the configuration file for the PCHID selected.

Edit source file

If you have exported your configuration file, you can use a workstation editor of your choice. Otherwise you can edit the file from the ***Edit source file*** panel. Here are the steps for editing a configuration file via the ***Edit source file*** panel.

Note: In order to make the edited source file the active configuration, you must import the source file (only if you are using a workstation editor and not the edit source file panel), validate the source file, and then activate it. For more

information about exporting, validating, and activating source files see, “Import source file” on page 36, “Validate source file” on page 47 and “Activate configuration” on page 48.

Steps for editing a source file:

1. From the ***OSC manual configuration*** panel select ***Edit source file***. Your source file will be displayed.
2. Make any necessary changes and save. For an example of a source file see, “Example of a correct configuration file.”
3. Validate your source file to check for any errors. If the file did not validate error free, the errors messages will appear directly in your source file. For an example of a source file with errors in it see, “Example of a configuration file with a warning” on page 41.

Sections of the configuration file

There are two sections to the session configuration file:

1. The first section is called the server section and includes parameters about the OSC as they relate to the OSA-Express card. In the file, the first line of the server section is the **<OSC_SERVER>** tag and the last line of the card parameters is the **</OSC_SERVER>** tag.

   Within the **<OSC_SERVER>** section of the file are the new dual-port physical port configuration parameters. Each set of port parameters begin with the **<OSC_PHYSICAL_PORT>** tag and ends with the **</OSC_PHYSICAL_PORT>** The index *x* is the index identifier of the physical port (0 or 1).
2. The second section includes parameters about the TN3270E sessions you want to configure for your OSA-ICC. You can configure up to 120 sessions on an OSA-ICC. In the file, the first line of the session parameters is the **<CONFIG_SESSION>** tag and the last line of the card parameters is the **</CONFIG_SESSION>** tag.

   Within the **<CONFIG_SESSION>** section of the file are the individual session configuration parameters. Each set session parameters begins with the **<SESSION*x*>** tag and ends with the **</SESSION*x*>** tag where *x* is the index number of the TN3270 session within the configuration. In addition to the previous session definition tags, the dual-port defined sessions contain a new IP_FILTER tag.

Example of a correct configuration file: The following is an example of a configuration file that matches the IOCP example given in this document.

```
<OSC_SERVER>
<OSC_PHYSICAL_PORT0>
  HOST_IP= 172.20.110.203
  SUBNET_MASK= 255.255.255.0
  PORT= 2300
  ETHERNET_FRAME= DIX
  MTU= 1492
  NAME= OSC_PORT_0
</OSC_PHYSICAL_PORT0>

<OSC_PHYSICAL_PORT1>
  HOST_IP= 173.20.110.204
  SUBNET_MASK= 255.255.255.0
  PORT= 1509
  ETHERNET_FRAME= DIX
  MTU= 1492
  NAME= OSC_PORT_1
</OSC_PHYSICAL_PORT1>
```

```
DEFAULT_GATEWAY= 172.20.110.2
</OSC_SERVER>

<CONFIG_SESSION>
<SESSION1>
  CSS= 03 IID= 02 DEVICE= 5400
  GROUP= "sess01"
  CONSOLE_TYPE= 1    RESPONSE= ON    READ_TIMEOUT= 300
  DEFER_HOST_DISCONNECT= 86400
  CLIENT_IP= 12.21.1.25
  IP_FILTER= 255.255.248.0
</SESSION1>

<SESSION2>
  CSS= 00 IID= 01 DEVICE= 5401
  GROUP= "sess02"
  CONSOLE_TYPE= 1    RESPONSE= ON    READ_TIMEOUT= 60
</SESSION2>

<SESSION3>
  CSS= 00 IID= 01 DEVICE= 5402
  GROUP= "sess03"
  CONSOLE_TYPE= 1    RESPONSE= ON    READ_TIMEOUT= 60
</SESSION3>
</CONFIG_SESSION>
```

Example of a configuration file with a warning: The following is an example of a configuration file that matches the configuration shown in the panels. The configuration file also includes a sample warning message that you would see after validating a file and receiving a warning.

```
<OSC_SERVER>

<OSC_PHYSICAL_PORT1>
  HOST_IP= 12.21.1.204
  SUBNET_MASK= 255.255.255.0
  PORT= 1509
  ETHERNET_FRAME= DIX
  MTU= 1492
  NAME= PortDefinition1
</OSC_PHYSICAL_PORT1>

  DEFAULT_GATEWAY= 12.21.1.2
</OSC_SERVER>

<CONFIG_SESSION>
<SESSION1>
// @@@ warning: This session is in Definition Error state
  CSS= 03 IID= 02 DEVICE= F400
  GROUP=  "sess01"
  CONSOLE_TYPE= 1    RESPONSE= ON    READ_TIMEOUT= 300
  DEFER_HOST_DISCONNECT= 86400
  CLIENT_IP= 12.21.1.25
  IP_FILTER= 255.255.248.0
</SESSION1>

<SESSION2>
  CSS= 00 IID= 01 DEVICE= 5401
  GROUP= "sess02"
  CONSOLE_TYPE= 1    RESPONSE= ON    READ_TIMEOUT= 60
</SESSION2>
</CONFIG_SESSION>
```

Configuration file syntax

The manual configuration file syntax includes the server and client tag identifiers and their corresponding values. These tags define the same parameters as the

Panel Entry input fields, although tag syntax may be slightly different from panel defined names. For example, ETHERNET_FRAME= defines the same parameter as Frame type in the panel. The format of the manual configuration file is as shown in "An example of a correct configuration file" in the previous page. The following general rules apply to tag placement:

1. Tags that are immediately followed by an equal sign (=) need associated values.
2. Non-delimiter tags may be abbreviated to a minimum of four characters.
3. Tags can be placed in any order given that they are within the bounds of their delimiters.
4. Server tags must be within the server delimiters.
5. Session tags must be within the Inner Session Delimiter and these inner delimiters must be within the Session Definition Delimiters.

The following is a list of the tags, delimiters and their descriptions.

Server tag identifiers

//	
<OSC_SERVER>	Server definition start delimiter
</OSC_SERVER>	Server definition end delimiter
<OSC_PHYSICAL_PORT#>	New physical port definition start delimiter
</OSC_PHYSICAL_PORT#>	New physical port definition end delimiter
HOST_IP=	
PORT=	
DEFAULT_GATEWAY=	
SUBNET_MASK=	
ETHERNET_FRAME=	
NAME=	
MTU=	

Client tag identifiers

<CONFIG_SESSION>	Session definition start delimiter
</CONFIG_SESSION>	Session definition end delimiter
<SESSION#>	Inner session definition start delimiter
</SESSION#>	Inner session definition end delimiter
CSS=	
MIFID= or IID=	
GROUP=	
CLIENT_IP=	
IP_FILTER=	
CONSOLE_TYPE=	
DEFER_HOST_DISCONNECT=	
RESPONSE=	
READ_TIMEOUT=	

Note: Any user-entered comment is erased during activation.

Server tag identifier descriptions:

// This indicates that any text at the end of the line is treated as a comment.

Note: Any user-entered comment is erased during activation.

<OSC_SERVER>
This tag indicates the beginning of the server configuration data. There can be only one such tag in the configuration file. It must be followed by the **</OSC_SERVER>** tag, or a syntax error is produced.

</OSC_SERVER>
This tag is the delimiter for the server configuration section. There can be only one such tag in the configuration file. It must be preceded by the **<OSC_SERVER>** tag, or a syntax error is produced.

<OSC_PHYSICAL_PORTx>
Marks the beginning of the individual physical port configuration; it must be followed by the **</OSC_PHYSICAL_PORTx>** tag. Everything between the **<OSC_PHYSICAL_PORTx>** and **</OSC_PHYSICAL_PORTx>** tags is treated as configuration data for one physical server port to which the client can connect. # is replaced by the corresponding index of the physical port value of 0 or 1. Each number can be used only once, since a physical port can be configured only once.

</OSC_PHYSICAL_PORTx>
Marks the ending of the individual physical port configuration; it must be preceded by the **<OSC_PHYSICAL_PORTx>** tag. Physical port tags within this boundary beginning with **<OSC_PHYSICAL_PORTx>** and ending with **</OSC_PHYSICAL_PORTx>** can be defined in any order. Each tag can appear only once for a particular physical port. They are followed by a number or string, which is assigned to a particular physical port parameter.

HOST_IP=
This tag is used to label the Host's IP address; a value that follows it should be an IP address in dotted format (for example, 10.10.12.43). This address is assigned to the OSA3270 server, and this is the address that TN3270E clients will be connecting to. The following is an example of using this tag: HOST_IP= 10.10.121.44. This tag is required for configuration and there is no default value.

PORT=
The port number on which the OSA3270 server will be listening (accepting) clients. For example, PORT= 3271. It is acceptable to use any valid port number in the integer range 1 to 65535. This is a required tag for server configuration.

DEFAULT_GATEWAY=
This value is used to specify the IP address, in dotted decimal format, of the default gateway (router) that will forward all traffic that is not destined to a local host residing on a network that one of the OSA-ICC ports is physically connected to. Only one Default Gateway can be specified for either single port, or dual-port deployments.

The DEFAULT_GATEWAY= tag is not required, if this tag is missing from the configuration file, the configuration validation will be successful and a default gateway value of 0.0.0.0 will be set. However, if the DEFAULT_GATEWAY= tag is present in the configuration file, then it must contain a dotted decimal IP address. If no IP address is present, then a validation syntax error will result

Please note that the IP address you specify will not be checked as part of the configuration validation operation to determine if the respective router is reachable via either OSA-ICC port. Therefore, you must ensure that the host at the respective address is not only reachable via one of the OSA-ICC ports, but that it will also satisfy your IP routing requirements.

The DEFAULT_GATEWAY= tag is the only server tag that is not included in the OSC_PHYSICAL_PORT boundary tags. Only one gateway is specified for both physical ports. The gateway tag must be within the OSC_SERVER boundary tag.

SUBNET_MASK=

The IP address in dotted decimal format for subnet mask. For example, SUBNET_MASK= 225.225.225.0. There is no default value; however it is an optional tag that will produce a warning if it is absent from the configuration file.

ETHERNET_FRAME=

Specifies the Ethernet standard that the network is defined to follow. Every host in a network must have the same frame type. The value can be DIX or SNAP.

This is a required tag for configuration it is defaulted to Default value: ETHERNET_FRAME= DIX

NAME=

The name can be up to 15 characters and is not case sensitive. Acceptable input characters include ASCII characters in the range given in Figure 29 on page 45. This tag is required for configuration and there is no default value.

Character	Dec	Oct	Hex	Character	Dec	Oct	Hex	Character	Dec	Oct	Hex
!	33	0041	0x21	A	65	0101	0x41				
"	34	0042	0x22	B	66	0102	0x42	a	97	0141	0x61
#	35	0043	0x23	C	67	0103	0x43	b	98	0142	0x62
$	36	0044	0x24	D	68	0104	0x44	c	99	0143	0x63
%	37	0045	0x25	E	69	0105	0x45	d	100	0144	0x64
&	38	0046	0x26	F	70	0106	0x46	e	101	0145	0x65
'	39	0047	0x27	G	71	0107	0x47	f	102	0146	0x66
(	40	0050	0x28	H	72	0110	0x48	g	103	0147	0x67
)	41	0051	0x29	I	73	0111	0x49	h	104	0150	0x68
*	42	0052	0x2a	J	74	0112	0x4a	i	105	0151	0x69
+	43	0053	0x2b	K	75	0113	0x4b	j	106	0152	0x6a
,	44	0054	0x2c	L	76	0114	0x4c	k	107	0153	0x6b
-	45	0055	0x2d	M	77	0115	0x4d	l	108	0154	0x6c
.	46	0056	0x2e	N	78	0116	0x4e	m	109	0155	0x6d
/	47	0057	0x2f	O	79	0117	0x4f	n	110	0156	0x6e
0	48	0060	0x30	P	80	0120	0x50	o	111	0157	0x6f
1	49	0061	0x31	Q	81	0121	0x51	p	112	0160	0x70
2	50	0062	0x32	R	82	0122	0x52	q	113	0161	0x71
3	51	0063	0x33	S	83	0123	0x53	r	114	0162	0x72
4	52	0064	0x34	T	84	0124	0x54	s	115	0163	0x73
5	53	0065	0x35	U	85	0125	0x55	t	116	0164	0x74
6	54	0066	0x36	V	86	0126	0x56	u	117	0165	0x75
7	55	0067	0x37	W	87	0127	0x57	v	118	0166	0x76
8	56	0070	0x38	X	88	0130	0x58	w	119	0167	0x77
9	57	0071	0x39	Y	89	0131	0x59	x	120	0170	0x78
:	58	0072	0x3a	Z	90	0132	0x5a	y	121	0171	0x79
;	59	0073	0x3b	[	91	0133	0x5b	z	122	0172	0x7a
<	60	0074	0x3c	\	92	0134	0x5c	{	123	0173	0x7b
=	61	0075	0x3d	]	93	0135	0x5d	|	124	0174	0x7c
>	62	0076	0x3e	^	94	0136	0x5e	}	125	0175	0x7d
?	63	0077	0x3f	_	95	0137	0x5f	~	126	0176	0x7e
@	64	0100	0x40	`	96	0140	0x60				

Figure 29. Valid characters for NAME= tag

MTU=

Specifies the maximum size to be transferred in one frame. A valid range is from 256–1492. A user would use an MTU size of less than 1492 when the routing equipment does not support anything above 576. This is a required tag for configuration. By default MTU is set to 1492.

Client tag identifier descriptions:

<CONFIG_SESSION>

Marks the beginning of the session configuration.

</CONFIG_SESSION>

Marks the end of the session configuration.

<SESSION#>

Marks the beginning of the individual session configuration; it must be followed by the </SESSION#> tag. Everything between the <SESSION#> and </SESSION#> tags is treated as configuration data for one session. # is replaced by the corresponding index of the session. This number is in the range 1-120. Each number can be used only once, since a session can be configured only once.

</SESSION#>

Marks the ending of the individual session configuration; it must be preceded by the <SESSION#> tag. Client tags (tags following this definition) within this boundary beginning with <SESSION#> and ending with </SESSION#> can be defined in any order. Each tag can appear only

once for a particular session. They are followed by a number or string, which is assigned to a particular session's parameter.

CSS= The channel subsystem number. The valid range is 0-3. This number is compared with IOCDS to make sure that it is defined. This tag is required for configuration and there is no default value.

MIFID= or IID=
The image ID for the session. The valid range is 1-F. This number is compared with IOCDS to make sure that it is defined. This tag is required for configuration and there is no default value.

DEVICE=
This is the device number associated to the session. This hexadecimal number will be compared with IOCDS to make sure that it is defined. The valid range is 0-65535. This tag is required for configuration and there is no default value.

GROUP=
Any valid ASCII characters except double quotes. The name must be included in double quotes. Acceptable input characters include ASCII values in the range displayed in Figure 30. This tag is required for configuration and there is no default value.

Character	Dec	Oct	Hex	Character	Dec	Oct	Hex	Character	Dec	Oct	Hex
!	33	0041	0x21	A	65	0101	0x41				
"	34	0042	0x22	B	66	0102	0x42	a	97	0141	0x61
#	35	0043	0x23	C	67	0103	0x43	b	98	0142	0x62
$	36	0044	0x24	D	68	0104	0x44	c	99	0143	0x63
%	37	0045	0x25	E	69	0105	0x45	d	100	0144	0x64
&	38	0046	0x26	F	70	0106	0x46	e	101	0145	0x65
'	39	0047	0x27	G	71	0107	0x47	f	102	0146	0x66
(	40	0050	0x28	H	72	0110	0x48	g	103	0147	0x67
)	41	0051	0x29	I	73	0111	0x49	h	104	0150	0x68
*	42	0052	0x2a	J	74	0112	0x4a	i	105	0151	0x69
+	43	0053	0x2b	K	75	0113	0x4b	j	106	0152	0x6a
,	44	0054	0x2c	L	76	0114	0x4c	k	107	0153	0x6b
-	45	0055	0x2d	M	77	0115	0x4d	l	108	0154	0x6c
.	46	0056	0x2e	N	78	0116	0x4e	m	109	0155	0x6d
/	47	0057	0x2f	O	79	0117	0x4f	n	110	0156	0x6e
0	48	0060	0x30	P	80	0120	0x50	o	111	0157	0x6f
1	49	0061	0x31	Q	81	0121	0x51	p	112	0160	0x70
2	50	0062	0x32	R	82	0122	0x52	q	113	0161	0x71
3	51	0063	0x33	S	83	0123	0x53	r	114	0162	0x72
4	52	0064	0x34	T	84	0124	0x54	s	115	0163	0x73
5	53	0065	0x35	U	85	0125	0x55	t	116	0164	0x74
6	54	0066	0x36	V	86	0126	0x56	u	117	0165	0x75
7	55	0067	0x37	W	87	0127	0x57	v	118	0166	0x76
8	56	0070	0x38	X	88	0130	0x58	w	119	0167	0x77
9	57	0071	0x39	Y	89	0131	0x59	x	120	0170	0x78
:	58	0072	0x3a	Z	90	0132	0x5a	y	121	0171	0x79
;	59	0073	0x3b	[	91	0133	0x5b	z	122	0172	0x7a
<	60	0074	0x3c	\	92	0134	0x5c	{	123	0173	0x7b
=	61	0075	0x3d	]	93	0135	0x5d	|	124	0174	0x7c
>	62	0076	0x3e	^	94	0136	0x5e	}	125	0175	0x7d
?	63	0077	0x3f	_	95	0137	0x5f	~	126	0176	0x7e
@	64	0100	0x40	`	96	0140	0x60				

Figure 30. Valid characters for GROUP= tag

CLIENT_IP=
This is the IP address that the client will use to connect to this session.

CLIENT_IP should be in a dotted decimal format, for example, 10.10.23.23; specifying a CLIENT_IP is optional. Omitting this tag however will allow any client to connect to a specific session. This tag is required for configuration and there is no default value.

CONSOLE_TYPE=
Specifies the session type: 1 (TN3270), 2 (master system operator console) or 3 (printer). The default configuration file should contain number descriptions in the comments next to the line with this tag. This is a required tag for configuration it is defaulted to: CONSOLE_TYPE= 1.

DEFER_HOST_DISCONNECT=
Indicates the amount of time to wait (in seconds) until the session tells the host you have disconnected. For example, if you wanted to turn your PC off without the host knowing you left, you would specify a value of 0. Then, DEFER_HOST_DISCONNECT will be enabled, but timeout for deferment will be infinity. The host will never be informed that you have logged off. For example, DEFER_HOST_DISCONNECT =0 If this tag is not used, then Defer Host Disconnect will be disabled for particular session. If value is specified, then it will be used as a deferment timeout parameter. For example, DEFER_HOST_DISCONNECT= 120 the valid range for this parameter is 1-86400. This tag is optional for file configuration, by default there is no DHD.

RESPONSE=
Response mode can be ON or OFF; that is, enabled or disabled. This tag is optional in file configuration, by default it is OFF. Recommended selection is ON.

READ_TIMEOUT=
Read timeout (RTO) is defaulted to 60 seconds, but if the user wishes to customize this parameter, they can do so by assigning number n to read timeout, as in READ_TIMEOUT= n. The valid range for n is 1-300 seconds. This tag is optional in file configuration.

Note: If no RTO is specified, Missing Interrupt Handler (MIH) should be disabled. If an RTO value is specified MIH should be set to at least 50% greater than the RTO value. MIH is set via the operating system.

IP_FILTER=
The IP_FILTER tag is similar to the network subnet mask; it defines a range of IP addresses that can connect to a given session. Clients requesting to connect that fit within the range of the IP_FILTER will be allowed to connect. Likewise clients with IP addresses outside this range requesting to connect will be refused a connection. The IP_FILTER is only applicable if the CLIENT_IP tag is specified. By default this tag is assigned the value 255.255.255.255, this is equivalent to specifying a unique client IP to the session definition.

Validate source file

Once you have edited a configuration file you must validate it in order to ensure that the file is valid before activating it. Here are the steps for validating a configuration file.

Warning: In order to make the validated source file the active configuration, you must activate it. Activating a configuration makes any changes you made effective immediately. This could result in active sessions being dropped. For more information about activating source files see “Activate configuration” on page 48.

Validating a manual configuration file

1. From the *OSC manual configuration* panel select *Validate source file* .
2. If the source file you are validating has errors or warnings, they will be included in comments in the source file. Only the first error will be detected. Therefore, you must fix that error and validate the source file again to determine if there are any additional errors. For an example of a source file with warnings in it, see "Example of a configuration file with a warning" on page 41. For a list of errors that you might receive, see Chapter 7, "Error and warning messages," on page 61. Here is the panel you will see if your source file has errors:

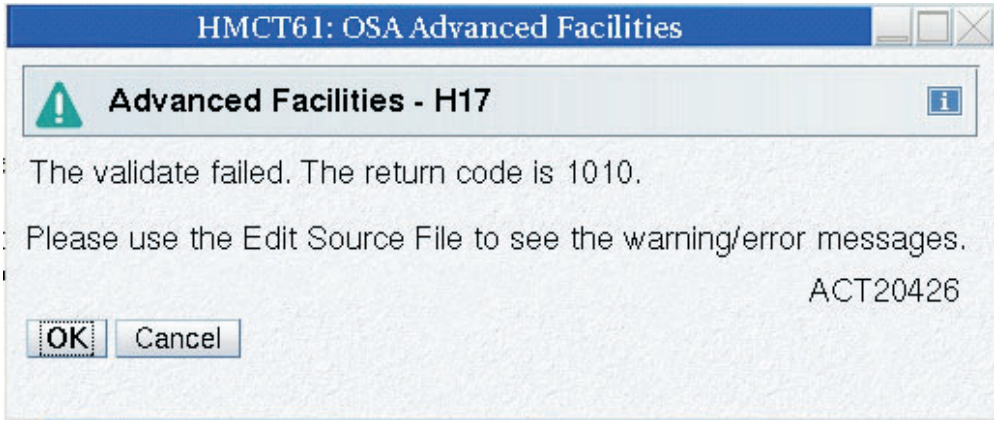

Figure 31. OSC validate source file panel

   You must fix all errors before activating your configuration. If you don't, you will receive the same errors while attempting to activate and your valid source file will be lost.
3. If the validate was successful, you will receive a message stating that validation of your source file was successful. Click OK.

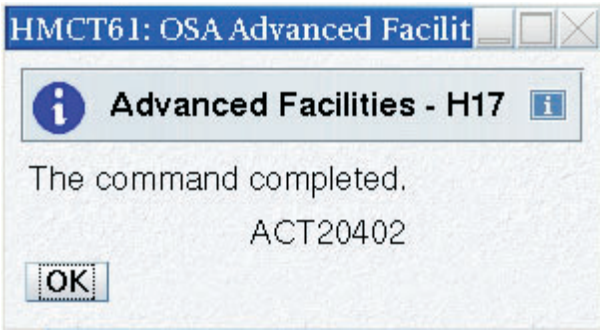

Figure 32. Successful validate source file

Activate configuration

The ***Activate configuration*** panel is used to activate a valid session configuration file. If you choose to activate a configuration file, your session will disconnect and then reconnect with the new configuration file option in effect.

Warning: You must validate the source file before you activate the configuration. Activating a configuration makes any changes made effective immediately. This could result in active sessions being dropped.

Note: You may want to export the configuration to save it as backup. For more information on exporting, see "Export source file" on page 37.

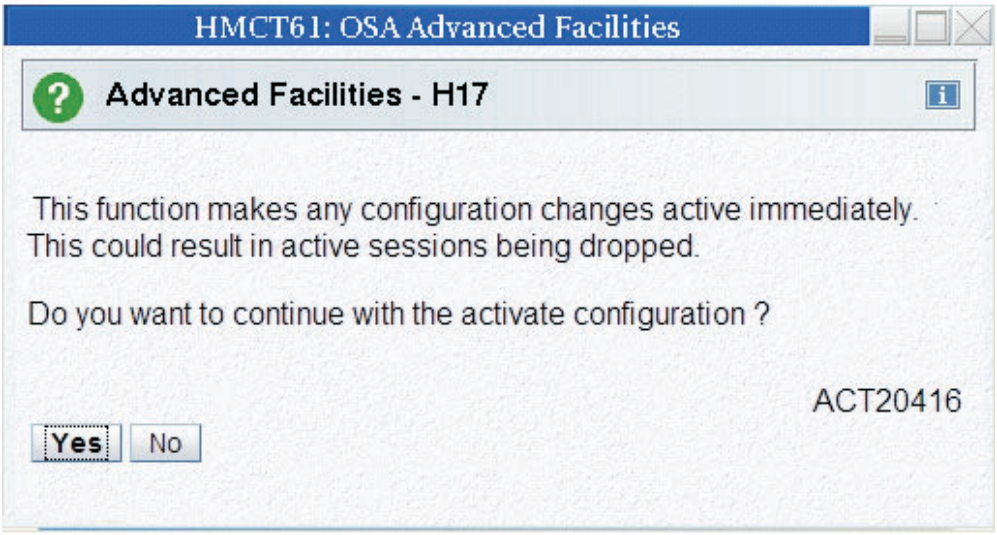

Figure 33. Activate configuration panel

Display activate configuration errors

The ***Display activate configuration errors*** panel is used to view the file which contains configuration error messages if any exist. If a configuration validated successfully, there are no activate configuration errors.

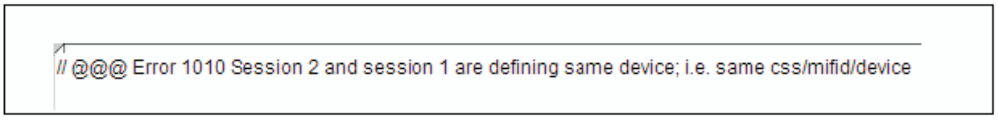

Figure 34. Display activate configuration errors panel

For a list of possible errors and warnings, see Chapter 7, "Error and warning messages," on page 61.

Debug utilities

The ***Debug utilities*** panel is the high level selection panel for the debug utilities that are used for debugging a problem with a session on an OSC.

To choose an OSC debug utility option, select a utility option and click OK.

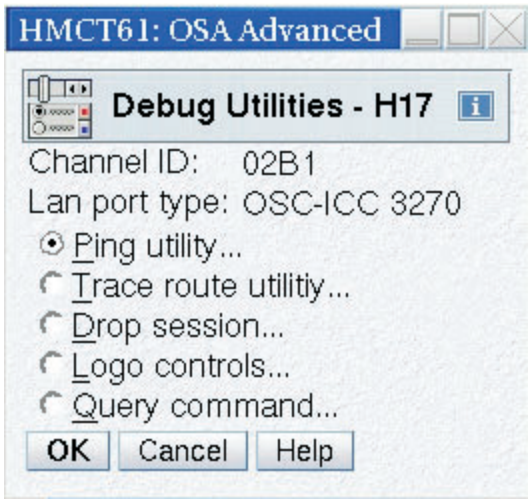

Figure 35. Debug utilities panel

Ping Utility

The ***Ping Utility*** panel is used to ping an active session to verify the status of the connection. A user can also ping the server's own IP address to verify the server's connection.

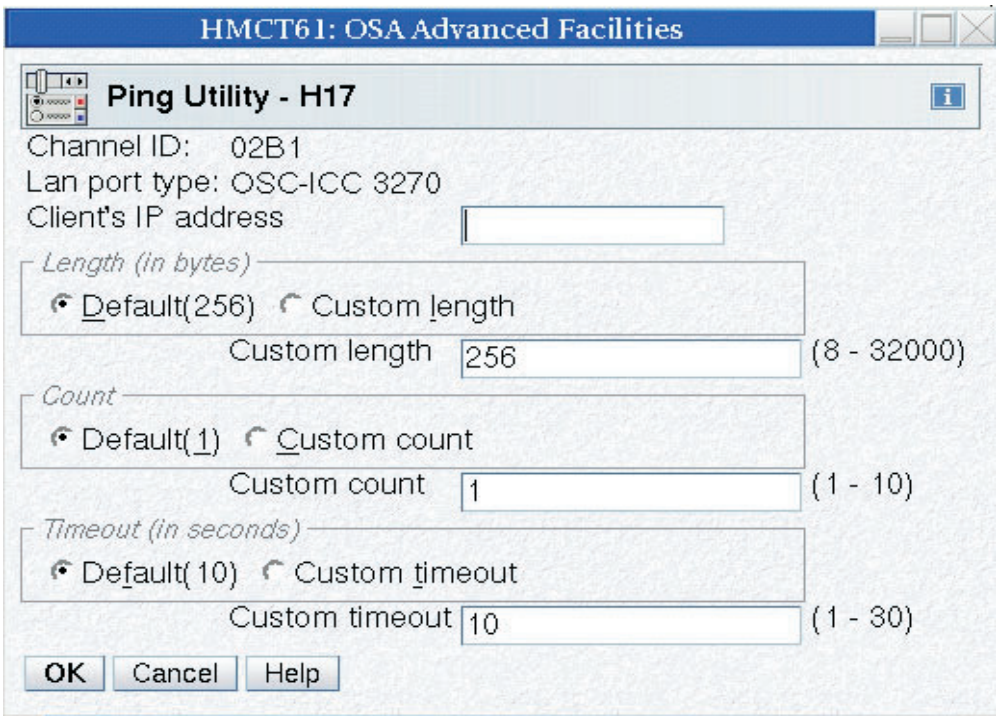

Figure 36. Ping Utility

The Ping utility requires the following input:

- Client's IP address: Specifies the IP address of the device you want to ping
- Length: You can select the default length of 256 bytes or enter a custom length of between 8 and 3200 bytes

- Count: You can select the default count of 1 or enter a custom count of between 1 and 10
- Timeout: You can select the default timeout value of 10 seconds or enter a custom timeout value.

Trace route utility

The ***Trace route utility*** panel is used to trace the route to the client interface specified by the IP address. The results of the trace route will give you every hop from OSA-ICC to the interface specified by the client's IP address.

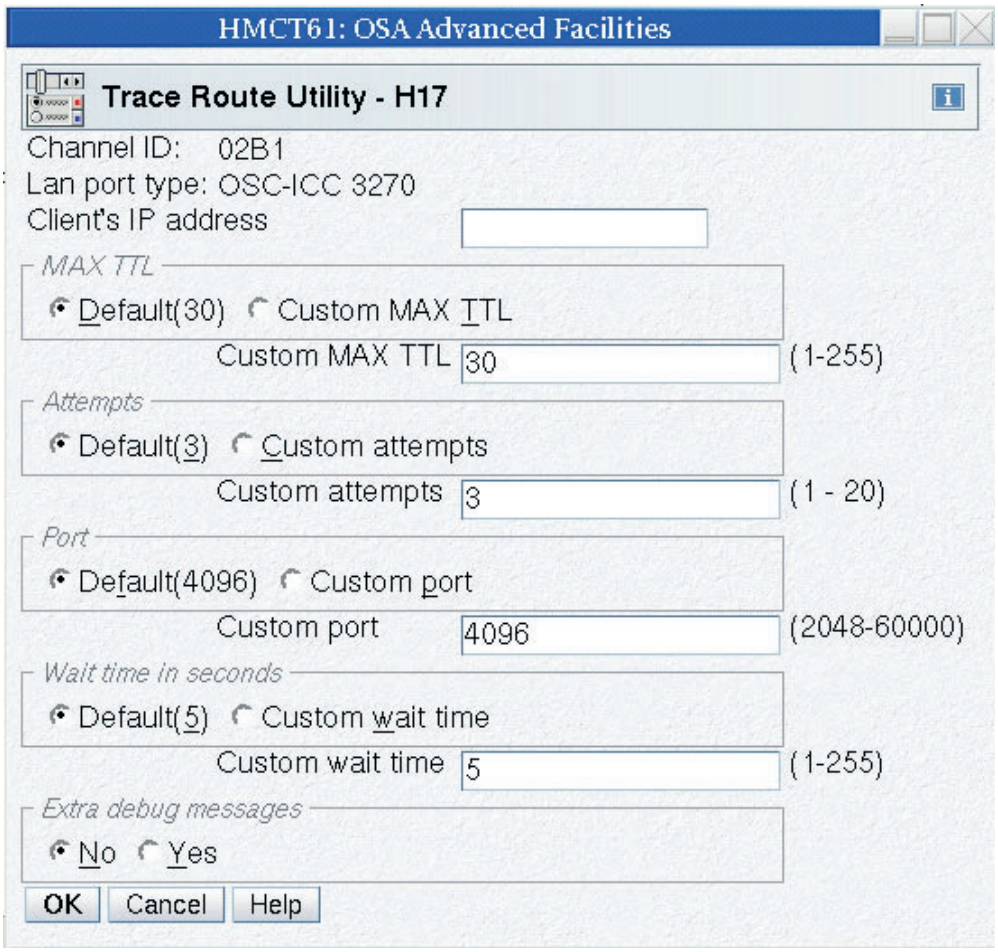

Figure 37. Trace route utility

The trace route utility requires the following input:

- Client's IP address: The IP address of the device you want to ping
- Max TTL: You can select the default maximum of 30 or enter a custom value of between 1 and 255
- Attempts: You can select the default number of attempts of 3 or enter a custom number of between 1 and 20
- Port: You can select the default port of 4096 or enter a custom port value of between 2048 and 60000
- Wait time in seconds: Specifies how long to wait for a trace route operation to complete.

- Extra Debug messages: If you select yes, extra debug messages are included in the result of the trace route.

Drop session

The ***Drop session*** panel is used to drop a session from an OSA-ICC. You can use this panel if you need to drop a session because you can't get to a PC or you have a bad connection.

If you selected auto-reconnect during the customization of your PCOMM session, drop session will not work. The auto-reconnect option will automatically reconnect your session after you drop it.

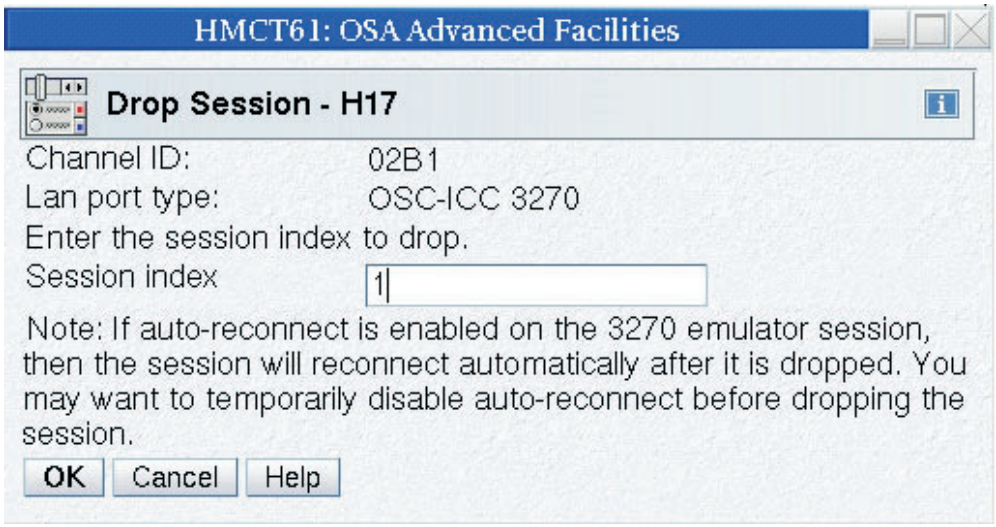

Figure 38. Drop session utility

The drop utility requires a session index number to identify which session to drop.

The drop session panel requires the following input:

- Session index: The index from the session table.

Logo Controls

The ***Logo Controls*** panel is used to enable or disable the 3 line logo (see page 56) that appears when the client console session is connected before traffic begins to flow.

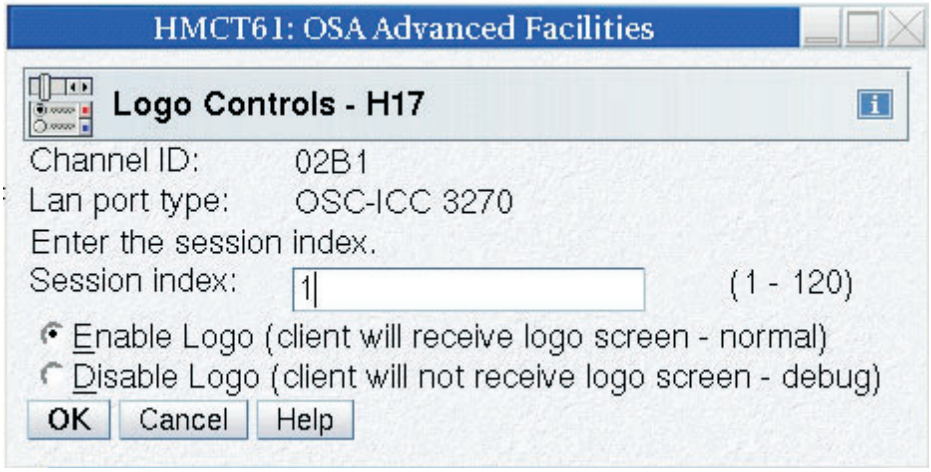

Figure 39. Logo Controls

The logo controls utility requires a session index from the session table number to identify which session's logo will be enabled or disabled.

The drop session panel requires the following input:

- Session index: The index from the session table.
- Button selection to Enable Logo or Disable Log

Query command

The ***Query Command utility*** panel is used as an informational query command interface to the OSA-ICC microcode. Information useful for troubleshooting can be queried via this function.

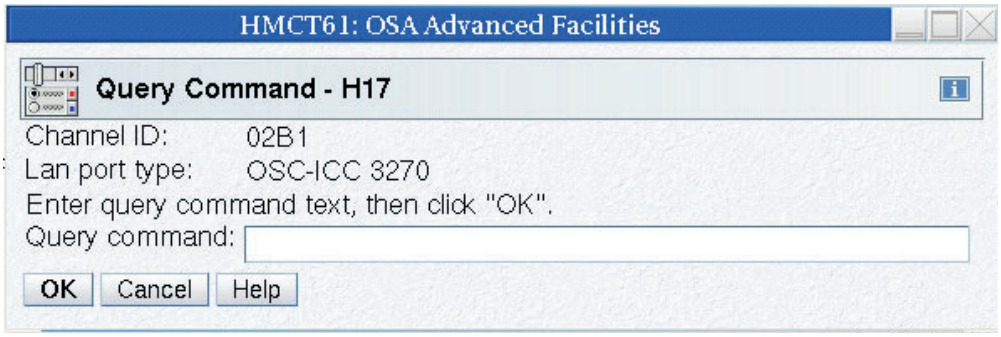

Figure 40. Query command

The query command utility requires an input command. Some commands may require additional input parameters. Enter `help` to view a list of currently supported commands. A supported command is further explained by entering `help` then the command name; an example is `help arp`. Some of the supported commands are **arp** and **route**. The results of a query command are displayed on a panel after successful execution of that command.

Cancel command

The ***Cancel Command utility*** panel allows you to cancel a command that is executing on an OSC.

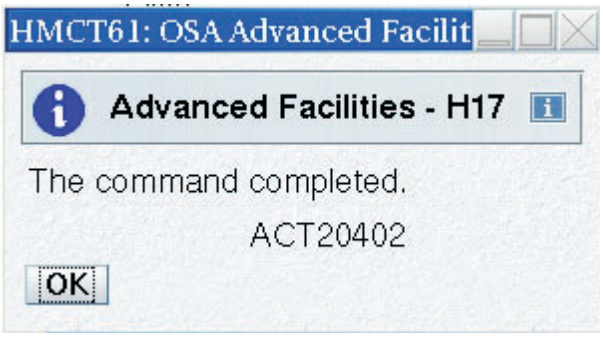

Figure 41. Cancel command panel

Chapter 5. OSA-ICC programming considerations

3270 Client Support

The **OSA-ICC** only supports TCP/IP RFC 2355 compliant Telnet TN3270E emulator programs, such as *IBM eNetwork Personal Communications*. These clients appear to the z/OS Operating System as non-SNA, DFT terminals. It does **not** support COAX attached clients. The OSA-ICC is essentially a control unit on a port of an OSA 1000BaseT Ethernet cards which controls up to 120 devices. In this document an OSA-ICC is referred to an OSC CHPID and each OSC can provide console support for any logical partition in any CSS on your z890 or z990 processor. The OSA-ICC configuration panels allow you to specify which logical partition on your processor each device is attached to using the CSS ID, MIF image ID, and device number.

The **3174** supports both COAX and LAN-attached, SNA and non-SNA, CUT and DFT mode terminals. It does ***not*** support TCP/IP attached clients. When configured in non-SNA, DFT mode, the 3174's 32 devices must all be assigned to a single logical partition on one specific S/390 or zSeries processor.

OSA-ICC does not support dynamic screen size terminal types (IBM_DYNAMIC). Using a client emulator that supports this terminal type and configuring sessions with the dynamic screen size may yield unpredictable and unexpected results if the session is connected to OSA-ICC.

Chapter 6. eNetwork Personal Communications Configuration

Below is an example of defining a PCOMM 3270 session. The example uses PCOMM version 5.6 for Windows. If you are using a different version, your panels may look slightly different.

When using IBM eNetwork Personal Communications (PCOMM) for client TN3270E display sessions, the following statement must be present in the PCOMM profile files (xxx.WS) to ensure that printer WCC controls are ignored if sent by the host:

```
[LT]
IgnoreWCCStartPrint=Y
```

If this statement is not present in your PCOMM profile files you will have to edit the xxx.WS files on your client PC with a PC text editor to add the statement lines.

Steps for customizing a PCOMM session

About this task

Procedure

1. To Define an Ethernet attached session to the host, click on 'Link Parameters.'

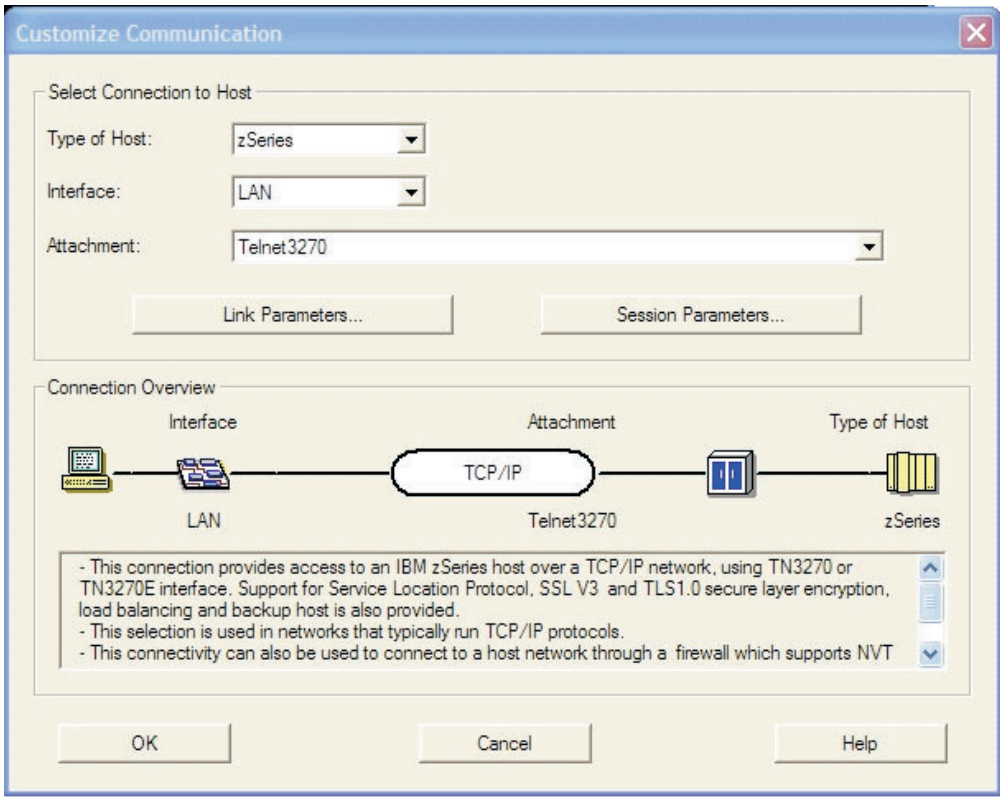

Figure 42. Customize communication screen

2. Define the connection from the workstation to the OSA-ICC server.

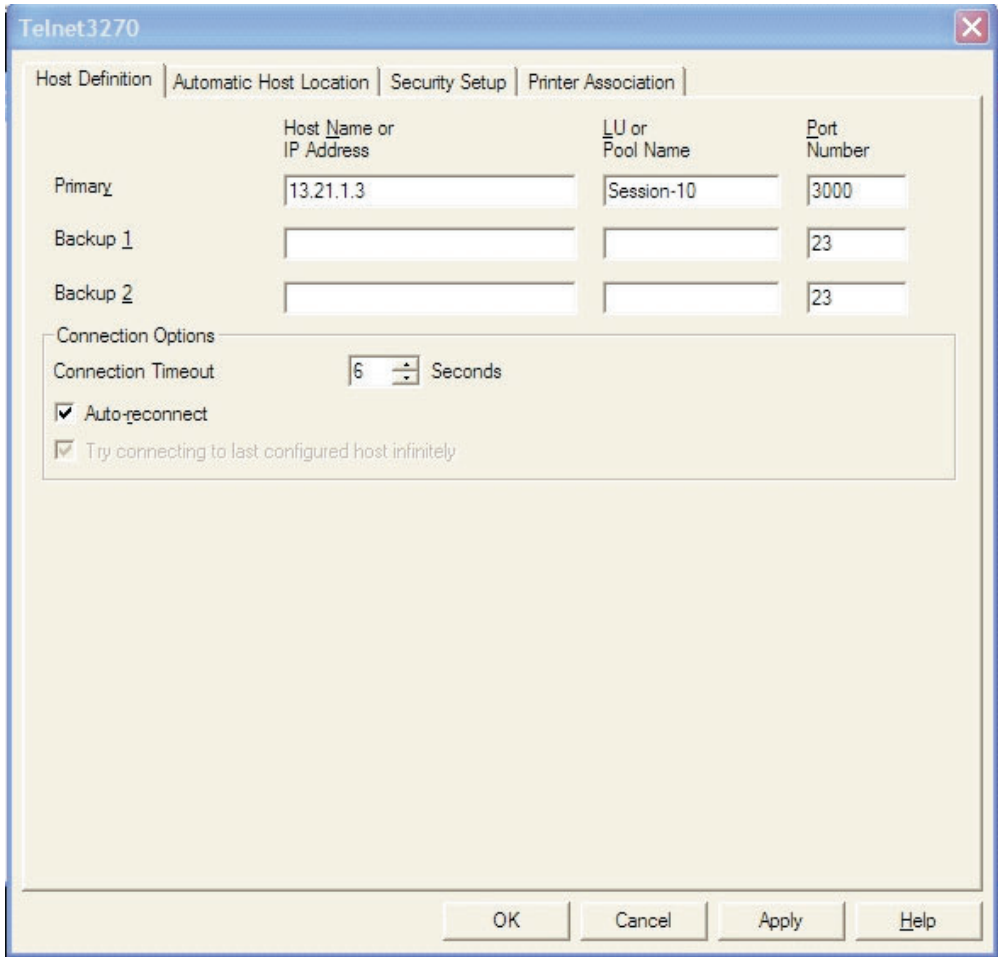

Figure 43. Telnet3270 screen

Enter the Host name or IP Address. The values in Host Name or IP Address and Port Number were specified when defining the OSA-ICC server configuration. For more information on defining your OSA-ICC server Configuration see, "Edit server configuration" on page 31.

---

3. Enter the LU or Pool Name. The value in LU or Pool Name was specified when defining the group name in the session configuration.

---

4. Enter the Port Number.

---

5. Click OK on the Telnet3270 panel.

Note: It is recommended that you select auto-reconnect. However, understand that the drop session option for configuring an OSA-ICC will not work. The auto-reconnect option will automatically reconnect your session after you drop it. For more information on the drop session option, see "Drop session" on page 52.

Results

If you wish, use the Session Parameters option in Customize Communication to set a screen size other than 24 by 80. It is recommended that your screen size matches the operating system screen size.

Note: OSA-ICC does not support dynamic screen size terminal types (IBM_DYNAMIC). Using a client emulator that supports this terminal type and configuring sessions with the dynamic screen size may yield unpredictable and unexpected results if the session is connected to OSA-ICC.

Clicking OK on the Customize Configuration panel causes PCOMM to initiate the connection to the host.

If the host session is not ready for communication, the screen displayed shows your connection information for this session. For example:

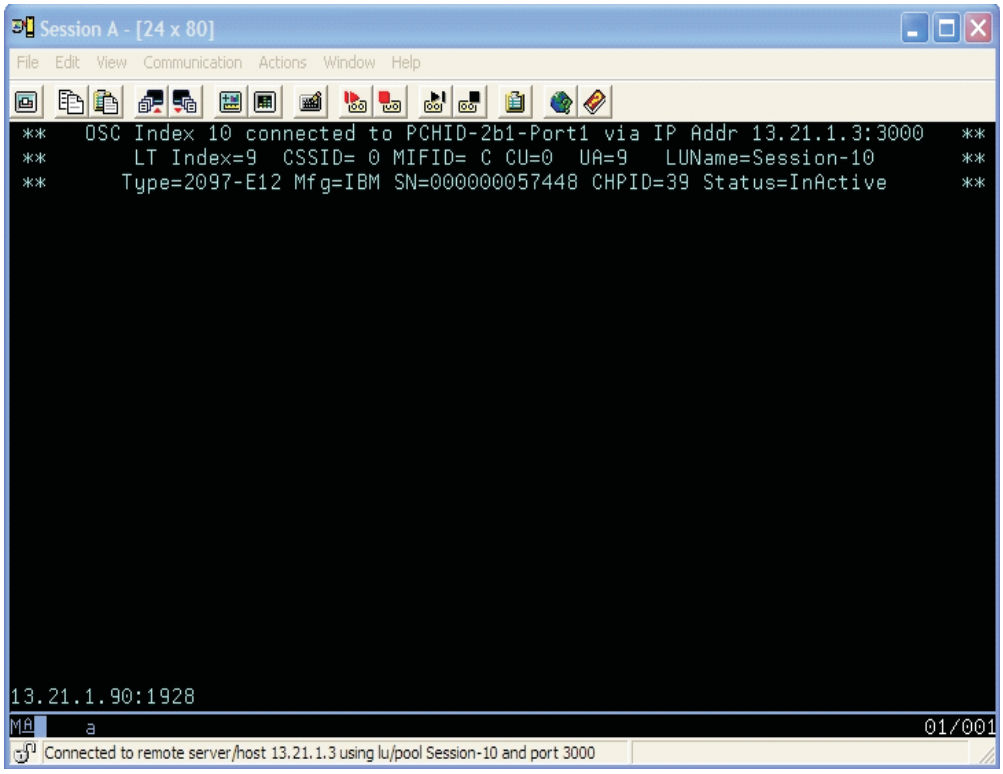

Figure 44. E - Capture — [24x80]

Line 1: OSAE000 is the defined server name; 13.21.1.3:3000 shows the defined server address and port number.

Line 2: session index; LCSS number; LPAR number (this is NOT the MIF image ID we specified for the session, but it is related); logical CU number (always 0); unit address for this device; LU name.

Line 3: information for the connected processor.

When using IBM eNetwork Personal Communications (PCOMM) for client TN3270E display sessions, the following statement must be present in the PCOMM profile files (xxx.WS) to ensure that printer WCC controls are ignored if sent by the host:

```
[LT]
IgnoreWCCStartPrint=Y
```

If this statement is not present in your PCOMM profile files you will have to edit the xxx.WS files on your client PC with a PC text editor to add the statement lines.

Chapter 7. Error and warning messages

By validating your configuration file, either by the ***Validate panel values*** panel or the ***Validate Source File*** panel, you are checking for any errors in your configuration. Any errors or warning you receive can be viewed in either the ***Display Validate panel values*** panel or in the source file as comments. Table 2 is a list of errors and warnings that you could receive:

Table 2. Errors from validate source file

Code	Text
1010	// @@@ error: Sessions X and Y are defining same device; i.e. same css/mifid/device
1020	// @@@ error: Can't have multiple <OSC_SERVER> tags
1021	// @@@ error: Can't have <OCS_SERVER> tag within session configuration
1022	// @@@ error: Card configuration already done
1030	// @@@ error: Illegal </OSC_SERVER> position
1031	// @@@ error: Server configuration section has to be closed by </OSC_SERVER>
1032	// @@@ error: Missing HOST_IP tag
1033	// @@@ error: Missing PORT tag
1034	// @@@ error: Missing DEFAULT_GATEWAY tag
1035	// @@@ error: Missing SUBNET_MASK tag
1036	// @@@ error: Missing ETHERNET tag
1037	// @@@ error: Missing NAME tag
1038	// @@@ error: Missing MTU tag
1039	// @@@ error: Can't have multiple HOST_IP tags
1040	// @@@ error: No host IP value
1041	// @@@ error: Can't have host IP outside of card configuration area
1042	// @@@ error: Host IP value is in bad format
1043	// @@@ error: Have to define host IP between <OSC_PHYSICAL_PORT#> and </OSC_PHYSICAL_PORT#> tags
1044	// @@@ error: Host name value is too long - 15 char is Max.
1045	// @@@ error: No host name value
1046	// @@@ error: Unsupported name format
1047	// @@@ error: Can't have name outside of card configuration area

Table 2. Errors from validate source file (continued)

1048	// @@@ error: Can't have multiple NAME tags
1049	// @@@ error: Have to define host name between <OSC_PHYSICAL_PORT#> and </OSC_PHYSICAL_PORT#> tags
1050	// @@@ error: No host port value
1051	// @@@ error: Can't have host port outside of card configuration area
1052	// @@@ error: Out of range port value
1053	// @@@ error: Can't have multiple PORT tags
1054	// @@@ error: Have to define host port between <OSC_PHYSICAL_PORT#> and </OSC_PHYSICAL_PORT#> tags
1055	// @@@ error: Host port value used for previous physical port definition
1056	// @@@ error: Host IP value used for previous physical port definition
1057	// @@@ error: Host IP for Physical Port 0 and Physical Port 1 are defined in the same segment
1060	// @@@ error: No gateway router value
1061	// @@@ error: Can't define gateway outside of the card configuration area
1062	// @@@ error: Invalid gateway address value or format
1063	// @@@ error: Can't have multiple DEFAULT_GATEWAY tags
1070	// @@@ error: No subnet mask value
1071	// @@@ error: Can't define subnet mask outside of the card configuration area
1072	// @@@ error: Invalid subnet address value or format
1073	// @@@ error: Can't have multiple SUBNET_MASK tags in card configuration area
1074	// @@@ error: Have to define host subnet mask between <OSC_PHYSICAL_PORT#> and </OSC_PHYSICAL_PORT#> tags
1080	// @@@ error: No value for Ethernet standard
1081	// @@@ error: Can't define Ethernet standard outside of card configuration
1082	// @@@ error: Unknown Ethernet standard value or format
1083	// @@@ error: Can't have multiple ETHERNET tags in card configuration area

Table 2. Errors from validate source file (continued)

1084	// @@@ error: Have to define host Ethernet standard between <OSC_PHYSICAL_PORT#> and </OSC_PHYSICAL_PORT#> tags
1090	// @@@ error: No value for MTU
1091	// @@@ error: Can't define MTU outside of card configuration
1092	// @@@ error: MTU value outside of 256-1492 range
1093	// @@@ error: MTU value has to be a decimal number
1094	// @@@ error: Can't have multiple MTU tags in card configuration area
1095	// @@@ error: Have to define host MTU between <> and <> tags
1100	// @@@ error: Can't have <CONFIG_SESSION> tag within card configuration area
1101	// @@@ error: Can't have multiple <CONFIG_SESSION> tags
1102	// @@@ error: Sessions configuration already done
1110	// @@@ error: Illegal </CONFIG_SESSION> position
1120	// @@@ error: <SESSION# needs to end with >, i.e.<SESSION#>
1121	// @@@ error: Trying to configure session outside of session configuration area
1122	// @@@ error: Session # is not between [1 and 120]
1123	// @@@ error: Overlapping configuration for different session
1124	// @@@ error: </SESSION# needs to end with >, i.e.</SESSION#>
1125	// @@@ error: Wrong session # in a </SESSION#> tag
1126	// @@@ error: This Session # has already been configured
1127	// @@@ error: Session # has to be a decimal number
1128	// @@@ error: This session is missing one of the mandatory tags : css, iid or device
1130	// @@@ error: Can't define CSS outside of session configuration area
1131	// @@@ error: Have to define CSS between <SESSION#> and </SESSION#> tags
1132	// @@@ error: Unsupported CSS value
1133	// @@@ error: CSS value is not present

Table 2. Errors from validate source file (continued)

1134	// @@@ error: Can't have multiple CSS tags in session configuration area
1140	// @@@ error: Can't define MIFID (IID) outside of session configuration area
1141	// @@@ error: Have to define MIFID (IID) between <SESSION#> and </SESSION#> tags
1142	// @@@ error: Unsupported MIFID (IID) value. Range is [01 - 0F].
1143	// @@@ error: MIFID (IID)value not present
1144	// @@@ error: Can't have multiple MIFID (IID) tags in session configuration area
1150	// @@@ error: Can't define device outside of session configuration area
1151	// @@@ error: Have to define device between <SESSION#> and </SESSION#> tags
1152	// @@@ error: Unsupported device value
1153	// @@@ error: Device value not present
1154	// @@@ error: Can't have multiple DEVICE tags in session configuration area
1160	// @@@ error: Can't define group name outside of session configuration area
1161	// @@@ error: Have to define group name between <SESSION#> and </SESSION#> tags
1162	// @@@ error: Unsupported group length
1163	// @@@ error: Group name value not present
1164	// @@@ error: Group name value not present or no quotes
1165	// @@@ error: Can't have multiple GROUP tags in session configuration area
1170	// @@@ error: Can't define client's IP outside of session configuration area
1171	// @@@ error: Have to define client IP between <SESSION#> and </SESSION#> tags
1172	// @@@ error: Client IP value in bad format
1173	// @@@ error: Client IP value not present
1174	// @@@ error: Can't have multiple IP_FILTER tags in session configuration area
1175	// @@@ error: Client mask selected bits are unsupported based on CIDR notation
1180	// @@@ error: Can't define type outside of session configuration area

Table 2. Errors from validate source file (continued)

1181	// @@@ error: Have to define console type between <SESSION#> and </SESSION#> tags
1182	// @@@ error: Undefined console type value
1183	// @@@ error: Console type value not present
1184	// @@@ error: Can't have multiple CONSOLE_TYPE tags in session configuration area
1190	// @@@ error: Can't define Defer Host Disconnect outside of session configuration area
1191	// @@@ error: Have to define Defer Host Disconnect between <SESSION#> and </SESSION#> tags
1192	// @@@ error: Value for a Defer Host Disconnect has to be a whole decimal number
1193	// @@@ error: Defer Host Disconnect value either too small or too large.
1194	// @@@ error: Defer Host Disconnect value not present
1195	// @@@ error: Can't have multiple DEFER_HOST_DISCONNECT tags in session configuration area
1200	// @@@ error: Can't define Response outside of session configuration area
1201	// @@@ error: Have to define Response between <SESSION#> and </SESSION#> tags
1202	// @@@ error: Unsupported value of Response
1203	// @@@ error: Response value not present
1204	// @@@ error: Can't have multiple RESPONSE tags in session configuration area
1210	// @@@ error: Can't define Read timeout outside of session configuration area
1211	// @@@ error: Have to define Read timeout between <SESSION#> and </SESSION#> tags
1212	// @@@ error: Read timeout value is too small. Range is (5-300]
1213	// @@@ error: Read timeout value is too large. Range is (0-300]
1214	// @@@ error: Read timeout value is not present
1215	// @@@ error: Read timeout value should be a whole decimal number

Table 2. Errors from validate source file (continued)

1216	// @@@ error: Can't have multiple READ_TIMEOUT tags in session configuration area
1221	// @@@ error:1221 LU (group) name has to be unique per partition (CSS.IID). LU names in sessions X and Y are in conflict.
1222	// @@@ error: 1222: Session IP has to be unique per partition (CSS.IID) when is used without Group (LU) name. IPs in sessions X and Yare in conflict.
1223	// @@@ error: 1223: When used in combination with the IP, LU name can't be used again, if it was already used in other session by it self. Sessions X and Y are in conflict.
1224	// @@@ error: 1224: Same LU name can't be used again, if it was already used in other session together with IP. Sessions X and Y are in conflict.
1225	// @@@ error: 1225: Neither group (LU) name nor IP is specified for session # X. At least one has to be specified
1283	// @@@ error: Server data must be defined before validation process
1290	// @@@ error: Illegal Token
1300	// @@@ error: Can’t define IP filter outside of session configuration area
1301	// @@@ error: Can't define IP filter without client IP
1302	// @@@ error: Have to define IP filter between <SESSION#> > and </SESSION#> > tags
1303	// @@@ error: IP filter value is in bad format
1304	// @@@ error: IP filter value not present
1305	// @@@ error: Can't have multiple IP_FILTER tags in session configuration area
1306	// @@@ error: Client mask has already been defined
1310	// @@@ error: <OSC_PHYSICAL_PORT# needs to end with >, i.e. <OSC_PHYSICAL_PORT#>
1311	// @@@ error: Trying to configure physical port outside of physical port configuration area
1312	// @@@ error: Physical port # is not between [0 and 1]
1313	// @@@ error: Overlapping configuration for different physical port

Table 2. Errors from validate source file (continued)

1314	/ @@@ error: <OSC_PHYSICAL_PORT# needs to end with >; i.e. </OSC_PHYSICAL_PORT#>
1315	// @@@ error: Wrong physical port # in a </OSC_PHYSICAL_PORT#> tag
1316	// @@@ error: This Physical port # has already been configured
1317	// @@@ error: Physical port # has to be a decimal number

Table 3. Warnings from validate source file

Code	Text
506	// @@@ warning: 506 This session is in Definition Error state because CSS is not defined in IOCDS
507	// @@@ warning: 507 This session is in Definition Error state because IID is not defined for CSS in IOCDS
508	// @@@ warning: 508 This session is in Definition Error state because Device is not defined for IID in IOCDS
509	// @@@ warning: 509 This session is in Definition Error state because device is not defined in IOCDS

Table 4. Errors from validate panels

Code	Text
1010	// @@@ Error 1010: Session # X and session # Y are defining same device; i.e. same css/mifid/device
1042	// @@@ Error 1042: Invalid server IP value:
1046	// @@@ Error 1046: Unsupported name format: XXXXX
1052	// @@@ Error 1052: Invalid server port value: XXXXX
1055	// @@@ Error 1055: Host port value used for previous physical port definition
1056	// @@@ Error 1056: Host IP value used for previous physical port definition
1057	// @@@ Error 1057: Host IP for Physical Port 0 and Physical Port 1 are defined in the same segment
1082	// @@@ Error 1082: Invalid server LAN PARM value: XXXXX
1092	// @@@ Error 1092: Invalid server MTU value: XXXXX
1132	// @@@ Error 1032 :Session # X has out of range CSS value.

Table 4. Errors from validate panels (continued)

1142	// @@@ Error 1042 :Session # X has out of range IID value.
1152	// @@@ Error 1052 :Session # X has out of range deviceNumber value.
1162	// @@@ Error 1162: Session #X has invalid group name length
1163	// @@@ Error 1163: Session #X has invalid group name
1172	// @@@ Error 1172: Session #X has invalid session IP value
1182	// @@@ Error 1082 :Session # X has invalid Type.
1202	// @@@ Error 1202 :Session # X has invalid RSP value.
1212	// @@@ Error 1212 :Session # X has invalid RTO value.
1221	// @@@ Error 1221 : LU (group) name has to be unique per partition (CSS.IID). LU names in sessions X and " Y are in conflict.
1222	// @@@ Error 1222 :Session IP has to be unique per partition (CSS.IID) when is used without Group (LU) name. IPs in sessions X and Y are in conflict.
1223	// @@@ Error 1223 :When used in combination with the IP, LU name can't be used again, if it was already used in other session by it self. Sessions X and Y are in conflict.
1224	// @@@ Error 1224: Same LU name can't be used again, if it was already used in other session together with IP. Sessions X and Y are in conflict.
1225	// @@@ Error 1225: Neither group (LU) name nor IP is specified for session # X. At least one has to be specified.
1303	// @@@ Error 1303 Session #X has invalid IP mask

Table 5. Warnings from validate panels

Code	Text
62	// @@@ Warning 62 :Invalid server gateway value: XXXXX
72	// @@@ Warning 72:Invalid server subnetMask value: XXXXX
506	// @@@ warning: Session X is in Definition Error state because CSS is not defined in IOCDS
507	// @@@ warning: Session X is in Definition Error state because IID is not defined for CSS in IOCDS

Table 5. Warnings from validate panels (continued)

508	// @@@ warning: Session X is in Definition Error state because device is not defined for IID in IOCDS
509	// @@@ warning: Session X is in Definition Error state because device is not defined in IOCDS

Appendix A. Network topology diagrams

Network topology diagram 1

In the topology diagram shown in Figure 45, there is no default gateway and both connections to OSA-ICC physical ports are private isolated subnets. When OSA-ICC dual-port connections are not routed, communication is available only to clients on the same subnet with the OSA-ICC physical port. Remote clients are not allowed to communicate with OSA-ICC.

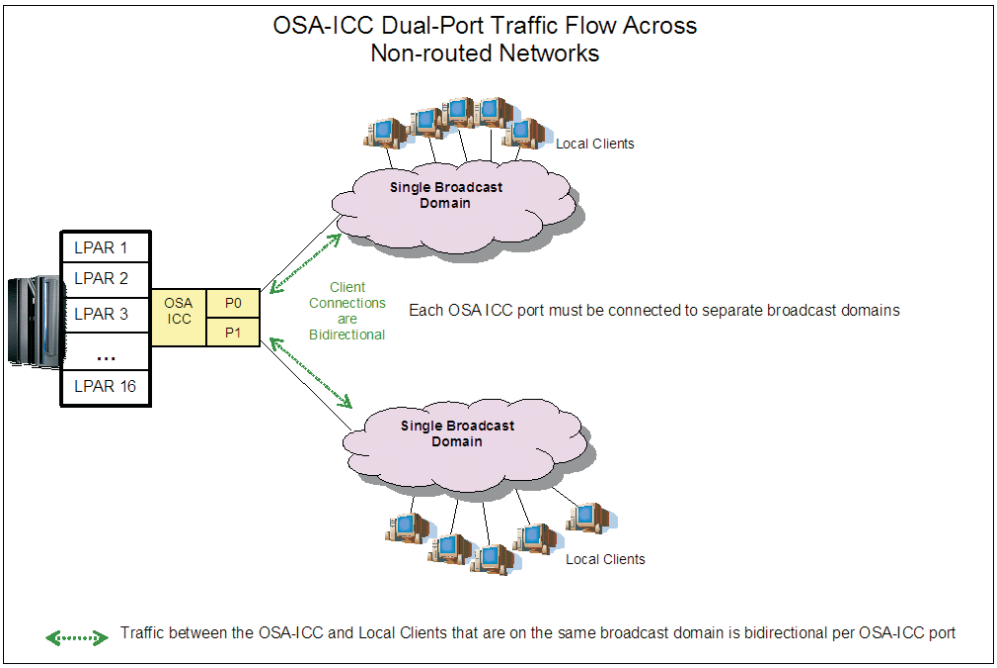

Figure 45. Network topology Diagram 1

Network topology diagram 2

In the topology diagram shown in Figure 46 on page 72, there is a local network attached to each physical port. This allows bidirectional communication with local clients and an OSA-ICC physical port connection. Remote clients can also communicate with OSA-ICC because there is an established path with the router. Although this path exists and allows inbound traffic, all outbound traffic is routed through Physical Port 0 because the default gateway resides on this subnet.

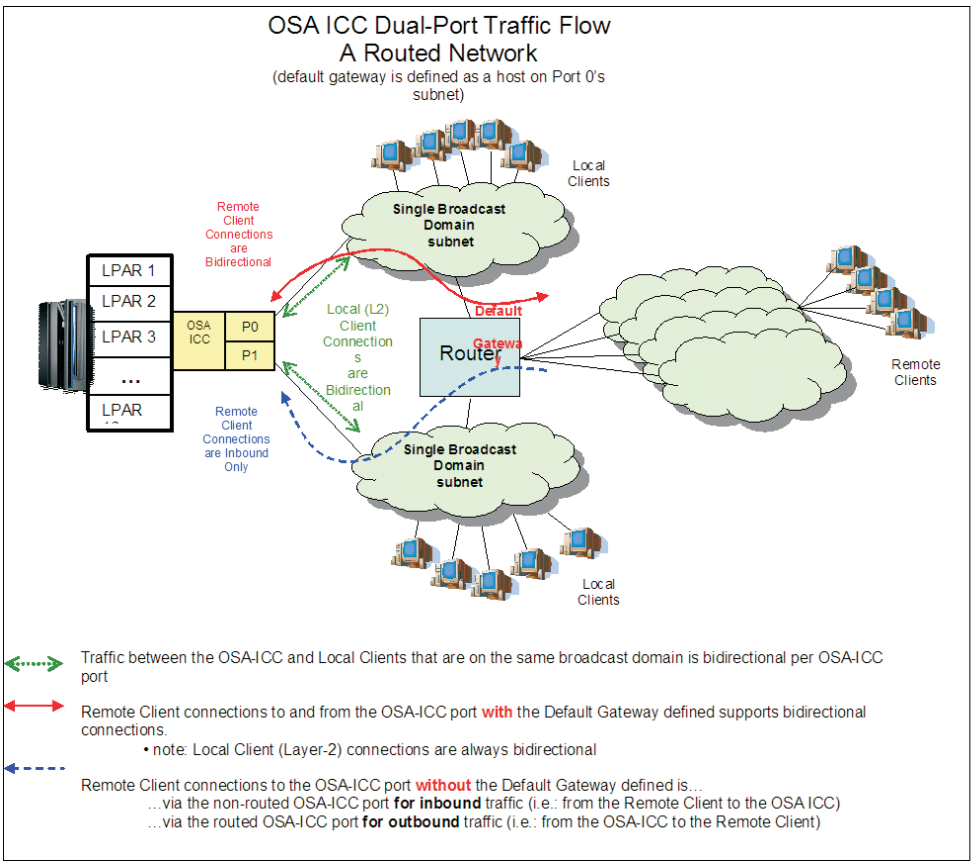

Figure 46. Network topology Diagram 2

Network topology diagram 3

In the topology diagram shown in Figure 47 on page 73, this network topology operates in a similar manner as the topology diagram shown in Figure 46. Instead of the default gateway being defined for the subnet of physical port 0 is defined for physical port 1. The same principle applies that remote clients can only access OSA-ICC from either port if they both have a connection to the router. However, outbound traffic is routed only through Physical Port 1 because this is the subnet on which the default gateway is defined.

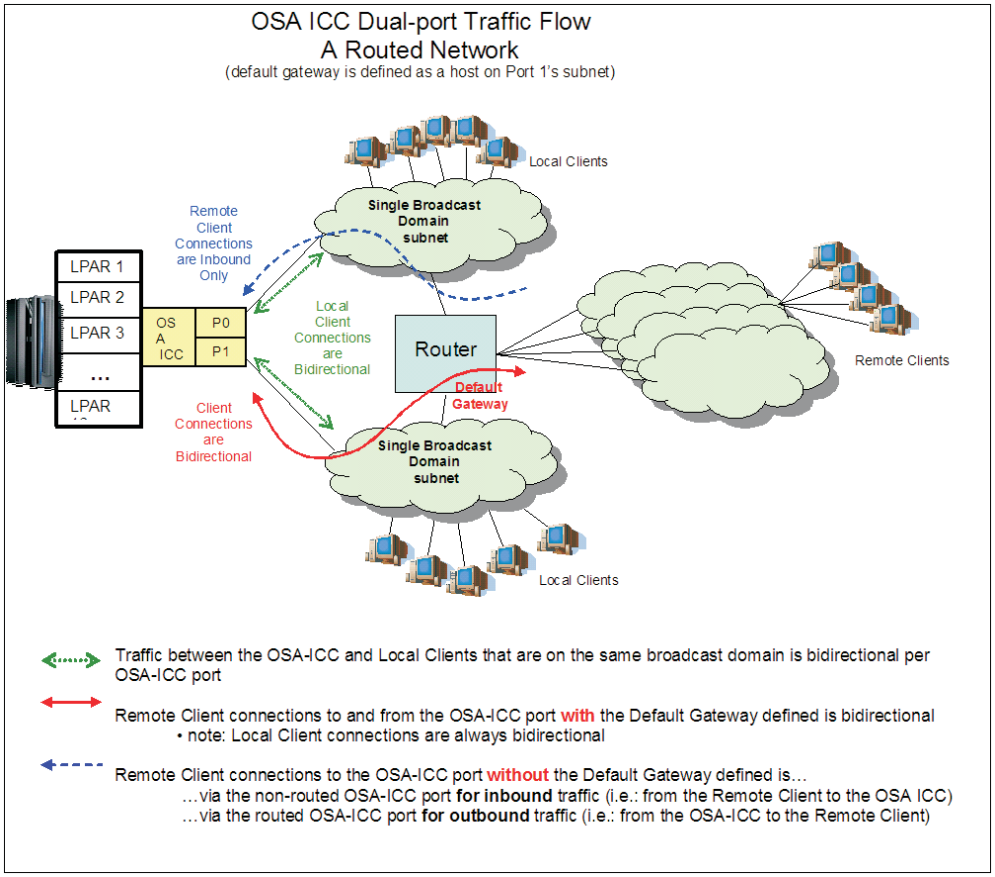

Figure 47. Network topology Diagram 3

Network topology diagram 4

In the topology diagram shown in Figure 48 on page 74, remote client connections to and from the routed OSA-ICC port (the port with the Default Gateway defined) are bidirectional unless the remote client resides on the same subnet as the non-routed OSA-ICC port.

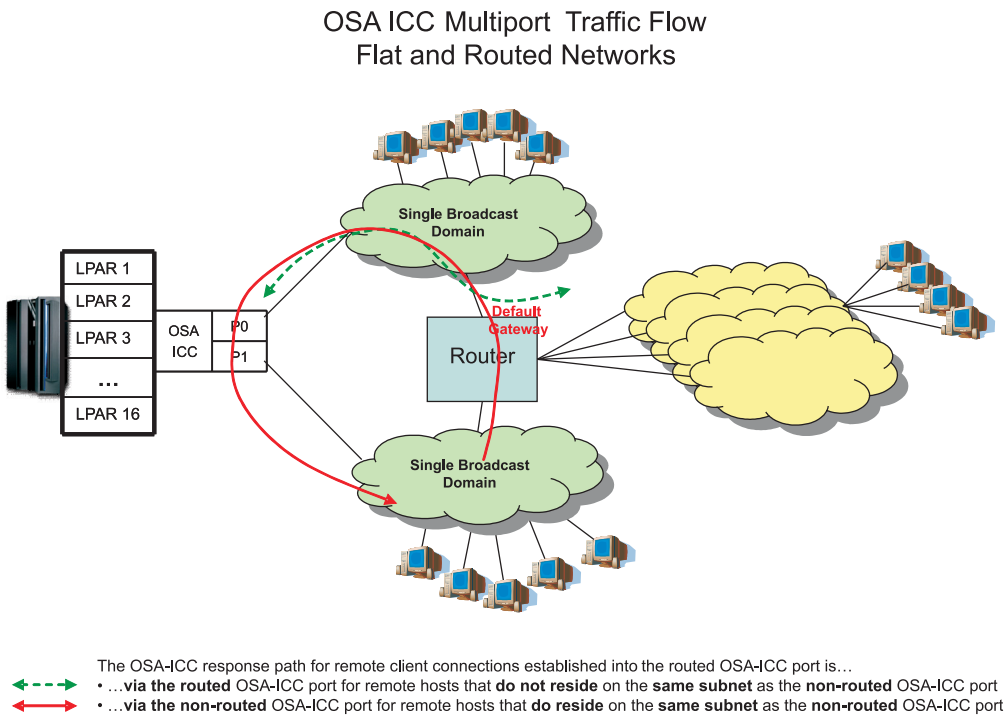

Figure 48. Network topology Diagram 4

Network topology diagram 5

The topology diagram shown in Figure 49 on page 75 is similar to that shown in Figure 48, where remote client connections to and from the routed OSA-ICC port (the port with the Default Gateway defined) are bidirectional unless the remote client resides on the same subnet as the non-routed OSA-ICC port.

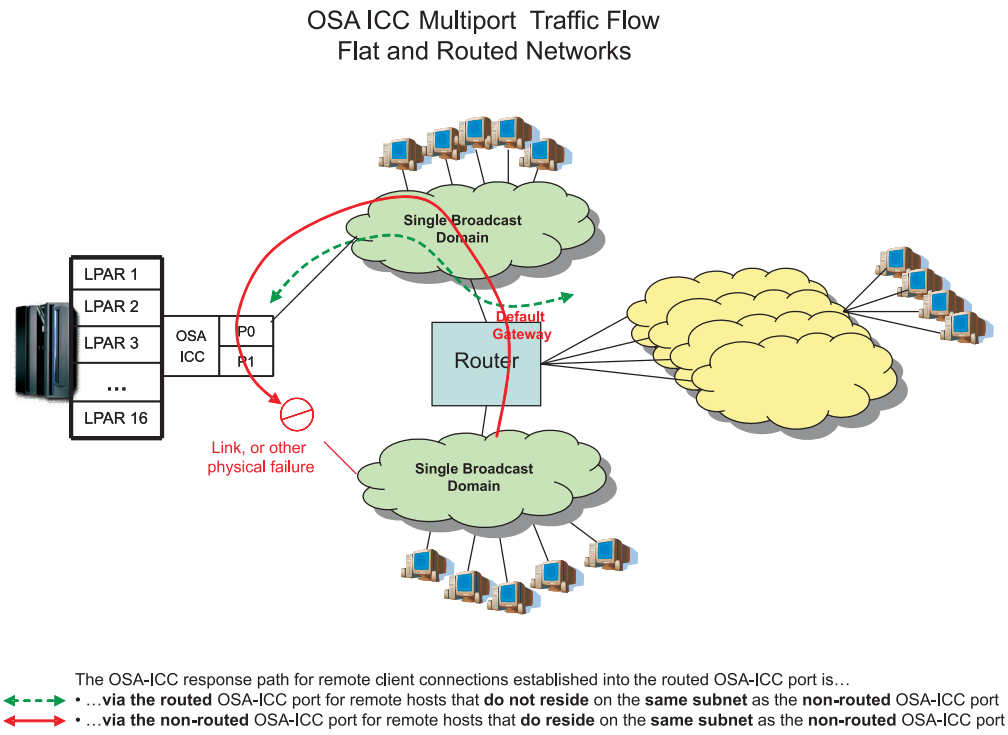

Figure 49. Network topology Diagram 5

Appendix B. Error codes that can be returned for an Advanced Facilities Function

Table 6 contains a list of error codes that can be returned for an Advanced Facilities Function. These errors pertain mainly to development and module communication, ensuring valid SE interface interaction; however some error codes may be encountered by the user. For panels related to validation process, Chapter 7, "Error and warning messages," on page 61 describes all the possible error codes.

Table 6. Error codes that can be returned for an Advanced Facilities Function

Error code	Description
5	The Write Per Subcommand attempts to transfer other than the record size
10	The Subcommand Count field is not 0
30	A command enabling execution of commands protected by the key counter was not already successfully executed in the CCW chain
32	Subcommand parameters 2-6 or 7 are non-zero
33	Subcommand parameters 0 bits 0-7 are non-zero
35	The address formed from the concatenation of SCP 0 and 1 is outside of any implemented OSA-3 channel address space
58	The LAN port parameter specified in subcommand parameter 1 may not be written
6D	The Diagnostic Function code is undefined
95	The LPRT index contained in subcommand parameter 0 is invalid
96	The port corresponding to the LPRT index contained in subcommand parameter 0 is not an implemented physical or logical port
9E	The class code contained in subcommand parameter 1 is invalid
A0 - A7	The port corresponding to the LAN port identifier contained in subcommand parameter 0 is not in the Disabled state
A9	The LAN port parameter specified in subcommand parameter 1 is invalid for the port type of the LAN port specified by the LPRT index contained in subcommand parameter 0
AA	The LAN port identifier contained in subcommand parameter 0 does not correspond to a physical port implemented in the current design

Table 6. Error codes that can be returned for an Advanced Facilities Function (continued)

Error code	Description
AB	A port diagnostic is currently in progress on some port in the OSA-3 channel
AC	Recovery code is currently executing on the specified port
AE	The function code is X'02' and the specified port does not use fiber optic technology
D0	The specified LAN port is in the Undefined state
D9	The specified LAN port is in the Unavailable state
DA	The specified LAN port is in the Definition Error state

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local laws:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names, which may be trademarks or service marks of others.

Index

Printed in USA

SA23-2266-02