z Systems

# *Open Systems Adapter Integrated Console Controller User's Guide*

SC27-9003-02

**Note**

Before using this information and the products it supports, read the information in “Notices” on page 109. 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, SC27-9003-02, refers to the IBM® Open Systems Adapter 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 SC27-9003-01.

There may be a newer version of this document in PDF format available on **Resource Link**. From the Resource Link home page (www.ibm.com/servers/resourcelink), 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).

Last updated: 2019-06-24

# Contents

# Figures

# Tables

# About this publication

This document describes the configuration process for the Open Systems Adapter Integrated Console Controller.

## Who should use this publication

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

## What is included in this publication

This publication contains the following chapters and appendixes:

- Chapter 1, “Open Systems Adapter Integrated Console Controller overview,” on page 1 is an introduction to the Open Systems Adapter-Express Integrated Console Controller.
- Chapter 2, “Server definition rules,” on page 3 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 to the system's hardware configuration,” on page 5 describes how to define your OSA-ICC PCHID to the system's hardware configuration.
- Chapter 4, “Displaying and managing OSA-ICC,” on page 11 describes the tasks for configuring your OSA-ICC.
- Chapter 5, “Configuring OSA-ICC ,” on page 27 shows how to use panel entries to configure your OSA-ICC.
- Chapter 6, “Manually configuring OSA-ICC,” on page 35 show how to manually configure your OSA-ICC.
- Chapter 7, “Debug utilities,” on page 49 shows such OSA-ICC utilities as Debug, Ping, and Trace Route.
- Chapter 8, “OSA-ICC TLS Encrypted Session Support,” on page 59 shows the ways to configure TLS on OSA-ICC.
- Chapter 9, “OSA-ICC programming considerations,” on page 75 provides brief programming tips for 3270 client support.
- Chapter 10, “eNetwork Personal Communications (PCOMM) configuration,” on page 77 provides an example of defining a PCOMM 3270 session.
- Chapter 11, “Error and warning messages,” on page 91 describes errors and warnings issued from the validate source file and validate panels.
- Appendix A, “ASCII table,” on page 103 displays an ASCII table.
- Appendix B, “Sample signed certificates,” on page 105 provides a sample certificate signing request and a sample self-signed certificate.
- Appendix C, “Network topology,” on page 107 provides a diagram and description of the OSA-ICC network topology.

## 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:

- IOCP User's Guide for ICP IOCP, SB10–7037
- HCD User’s Guide, SC33-7988

## 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:

**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-Express features and may refer to OSA-Express as OSA.

**OSA-Express**
Abbreviation for Open Systems Adapter-Express features.

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

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

**TLS**
Transport Layer Security.

# How to send your comments to IBM

We invite you to submit comments about the z/OS® product documentation. Your valuable feedback helps to ensure accurate and high-quality information.

**Important:** If your comment regards a technical question or problem, see instead “If you have a technical problem” on page xv.

Submit your feedback by using the appropriate method for your type of comment or question:

**Feedback on z/OS function**
If your comment or question is about z/OS itself, submit a request through the IBM RFE Community (www.ibm.com/developerworks/rfe/).

**Feedback on IBM Knowledge Center function**
If your comment or question is about the IBM Knowledge Center functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Knowledge Center Support at ibmkc@us.ibm.com.

**Feedback on the z/OS product documentation and content**
If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to mhvrcfs@us.ibm.com. We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:

- Your name, company/university/institution name, and email address
- The following deliverable title and order number: OSA-ICC User's Guide, SC27-9003-02
- The section title of the specific information to which your comment relates
- The text of your comment.

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

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

## If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:

- Go to the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

# Summary of changes

Changes have been made to this document.

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 each change.

## Summary of changes for SC27-9003-01

This version has received editorial and terminology updates.

Extensive changes and additions were made to Chapter 8, “OSA-ICC TLS Encrypted Session Support,” on page 59.

# Chapter 1. Open Systems Adapter Integrated Console Controller overview

The IBM Open Systems Adapter Integrated Console Controller (OSA-ICC) provides tn3270e connectivity to non-SNA DFT 3174-type host connections. The OSA-ICC 3270 sessions allow you to IPL your logical partitions within any channel subsystem (CSS) and provides System Operator/Master consoles for z/OS, z/VM®, and z/VSE. The defined OSA-ICC sessions can also be used by TSO, VM, or VSE system programmers as standard tn3270e consoles.

Each OSA-ICC is capable of handling 120 sessions. The OSA-ICC uses TCP/IP connections over an Ethernet LAN to attach to workstations that are running an RFC 2355 compliant TN3270E emulator.

New for z13 (D27K MCL P08440.002) and above is the introduction of Transport Layer Security (TLS) encrypted session support. Specifically designed for Master Consoles, this support can also provide encryption for your standard TSO-like sessions. The new function provides the capability to support 48 concurrent TLS sessions through a single OSA-ICC adapter.

IBM has tested the Host Access Client Package which includes the eNetwork Personal Communications emulator (PCOMM) Level 20150317 S and above. For other tn3270e emulator questions, contact the emulator's product vendor directly for terms, conditions, prices and other product details.

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 windows are accessible on your Hardware Management Console and your Support Element (SE) console. These windows allow you, the system programmer, to customize each OSA-ICC on your system.

## Planning considerations

### Redundancy

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 support

Newly added with z13 (D27K MCL P08440.002) and above is the ability to connect console clients to the ICC securely, using Transport Layer Support (TLS) as the connection protocol. TLS and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. With OSA-ICC TLS support, the requirement for an external VPN to provide security is no longer necessary.

The CP Assist for Crypto Functions (CPACF) must be installed and enabled before the OSA-ICC TLS support can be configured and enabled. You can verify the function by checking the CPC Status Page (Figure 1 on page 2).

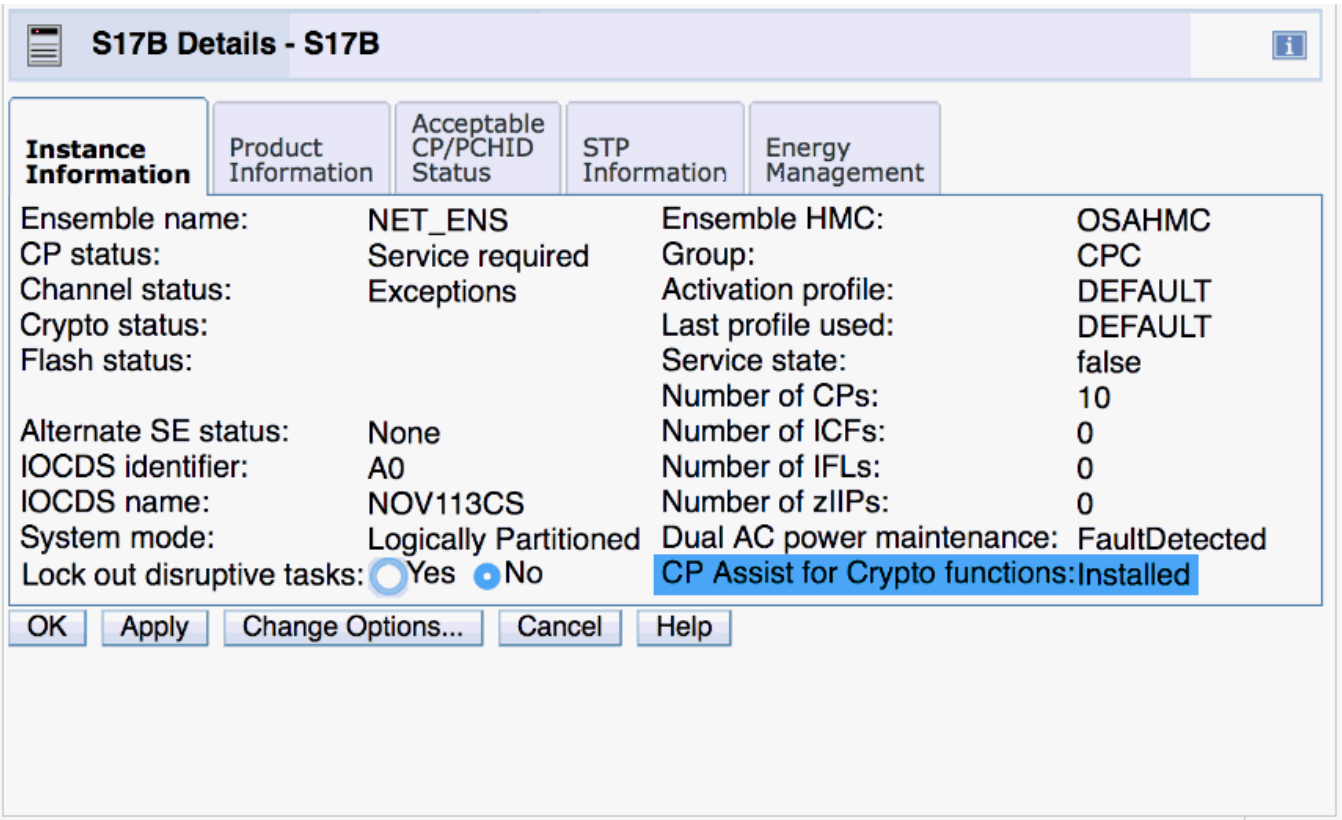



*Figure 1. CPC status page (CP Assist for Crypto functions highlighted)*

## Certificate and key management

Limited OSA-ICC TLS key management is provided. A single key, self-signed X.509 certificate, and certificate request is stored on the password protected SE and in the configuration information stored on the OSA adapter. We expect the customer to manage and secure additional certificates if required.

The certificate and key are protected by checksum and date on the closed SE system. The checksum and date are verified every time the key/certificate is loaded by the OSA-ICC adapter.

When creating or importing certificates, the strength of the allowed private key is fixed by firmware. The files are stored in PEM format. Digital signatures are generated using RSA.

## Recommended PCOMM levels

Recommended PCOMM levels for OSA-ICC:

- PCOMM Level 6.014, dated 20150317 S for non-TLS Sessions
- PCOMM Level 6.016, dated 20151006 S for TLS Sessions

| **Note:** |
| --- |
| Users at lower levels might experience unstable connections that repeatedly drop and recover when used with OSA-ICC cards on z13s processors. |

# Chapter 2. Server definition rules

OSA-ICC server rules include the following:

- Unique TCP Port number for each physical port
- Unique secure TCP Port number for each physical port
- Different subnet for each physical port host IP
- Single defined common gateway

## Client connection rules

When a client is connecting to the OSA-ICC, the client gets assigned a session number based on what is in the client session table. If the client does not meet the criteria described later in this section, or there are no more free sessions, that client's connection attempt is refused.

Two rules define connections:

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

Two inputs to the session table:

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

The session table has the following rules (configured via panels or via manually edited source file):

- Each session must contain at least one of the following element:.
  - Session LU name
  - IP address
- A session can contain both a client’s IP and a session 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 can not have that same LU name without also specifying an 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.

**Client assignment hierarchy**:

- 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, then the IP address of the incoming client has no meaning.
- 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 or non-matching LU or defined in multiple CSS/image | No Connection |
| 4 | LU name and client IP address specified | Good LU, good IP | Connection |
| | | Good LU, non-matching Client IP | No connection |
| | | No or non-matching LU, matching Client IP | No connection |
| | | No or non-matching LU, matching Client IP | No connection |
| | | No or non-matching LU, matching Client IP | No connection |
| | | No or non-matching LU, matching Client IP | 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/non-matching IP or defined in multiple CSS/images | No connection |

# Chapter 3. Defining your OSA-ICC to the system's hardware configuration

To use an OSA Card as an OSA-ICC adapter, the OSA-Express channel must be defined as an OSC CHPID. In order for your system to recognize an OSC CHPID, you must define the CHPID in your Input/Output Configuration Dataset (IOCDS) via the Hardware Configuration Definition (HCD) tool, or the Input/Output Configuration Program (IOCP).

Each OSA-ICC feature requires a unique CHPID, control unit, and device range definition. A OSC CHPID cannot be defined to span control units.

Although only 120 devices (sessions) can be configured on the ICC card at one time, the IOCDS definitions can contain more than 120 configurable devices.

## Defining an OSC CHPID via IOCP

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 6.

```
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 OSA-Express 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 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 USB device or transfer to a server via ftp/sftp. 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**

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 5.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.

```
                          z/OS V2.2 HCD
Command ===>

                              Hardware Configuration

Select one of the following.

__   0.  Edit profile options and policies
     1.  Define, modify, or view configuration data
     2.  Activate or process configuration data
     3.  Print or compare configuration data
     4.  Create or view graphical configuration report
     5.  Migrate configuration data
     6.  Maintain I/O definition files
     7.  Query supported hardware and installed UIMs
     8.  Getting started with this dialog
     9.  What's new in this release

For options 1 to 5, specify the name of the IODF to be used.

I/O definition file . . .  'IODFST.IODFD7'                              +
```

*Figure 2. Hardware configuration main menu*

_____

2. Select 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
   - Channel ID
   - 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 window. 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. With the introduction of z/OS V2R1, you can now add and delete CONSOLE definitions dynamically.
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

## IOCP statements

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. Displaying and managing OSA-ICC

Before you can connect any TN3270E session to the ICC, the OSA Adapter must be online to the Hardware Management Console or the Support Element (SE).

## Hardware Management Console and Support Element console

You can manage your OSA-ICC from the Advance Facilities window which is accessible from either your Hardware Management Console (HMC) or your Support Element (SE) console. These two consoles are the only way you can access the OSA-ICC configuration windows. For more information on these consoles, see the content in the SE and HMC (Version 2.12.1) publications, which has been incorporated into the help information. This information is located from the SE and HMC. You can also access this help information from IBM Knowledge Center (www.ibm.com/support/knowledgecenter).

## Steps for accessing the Advanced Facilities window

**About this task**

This manual assumes that the user has a basic understanding of how to access and manage their system using the SE or HMC.

Before you can connect any TN3270E session to the ICC, the OSA Adapter must be online to the partition.

**Note:** This section shows examples of using the Hardware Management Console and the SE, because the initial windows to select the PCHID are different.

Be aware of the following OSA-ICC initialization time delays:

1. OSA ICC initialization: 20-25 seconds; therefore, wait 20 - 25 seconds before performing config off or any other SE panel operations.
2. CEC Activate: Wait for 20-25 seconds after active message completion before performing CEC deactivate.

### Accessing the Advanced Facilities window from the HMC

**Procedure**

1. From the Hardware Management Console workplace window, click **Tasks Index** on the left-hand navigation pane.

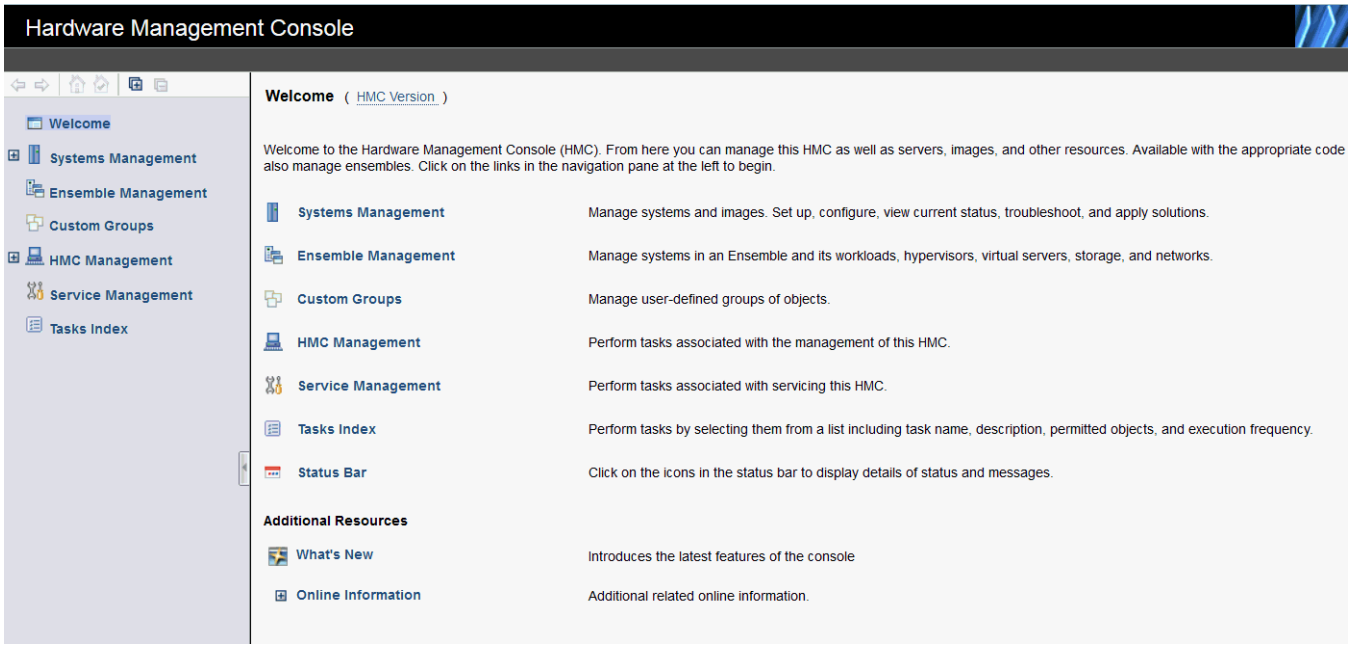



*Figure 3. Hardware Management Console workplace window*

2. From the Tasks Index, click **OSA Advanced Facilities**.
3. The OSA Advanced Facilities window opens. Select the PCHID you wish to configure and select OK.

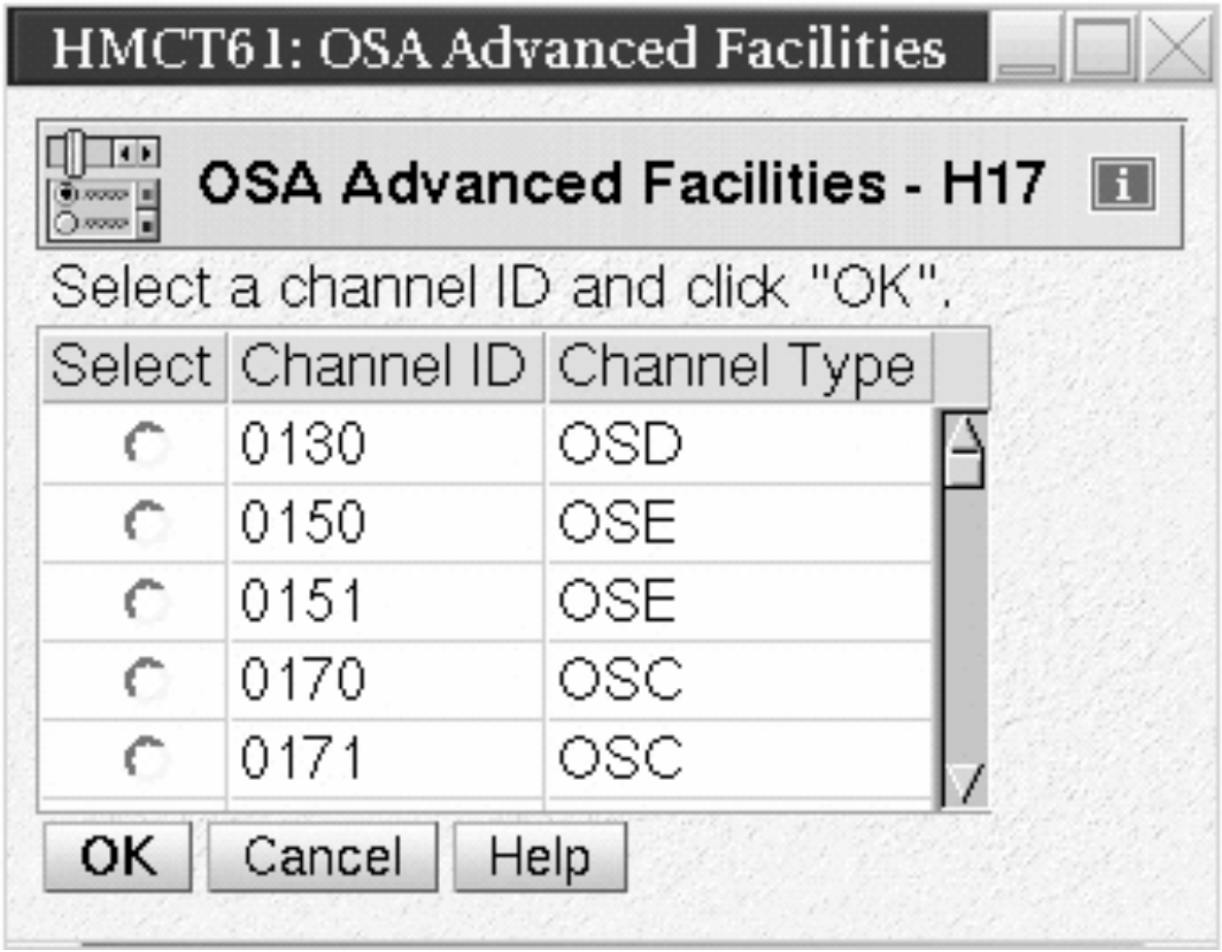



*Figure 4. OSA Advanced Facilities window*

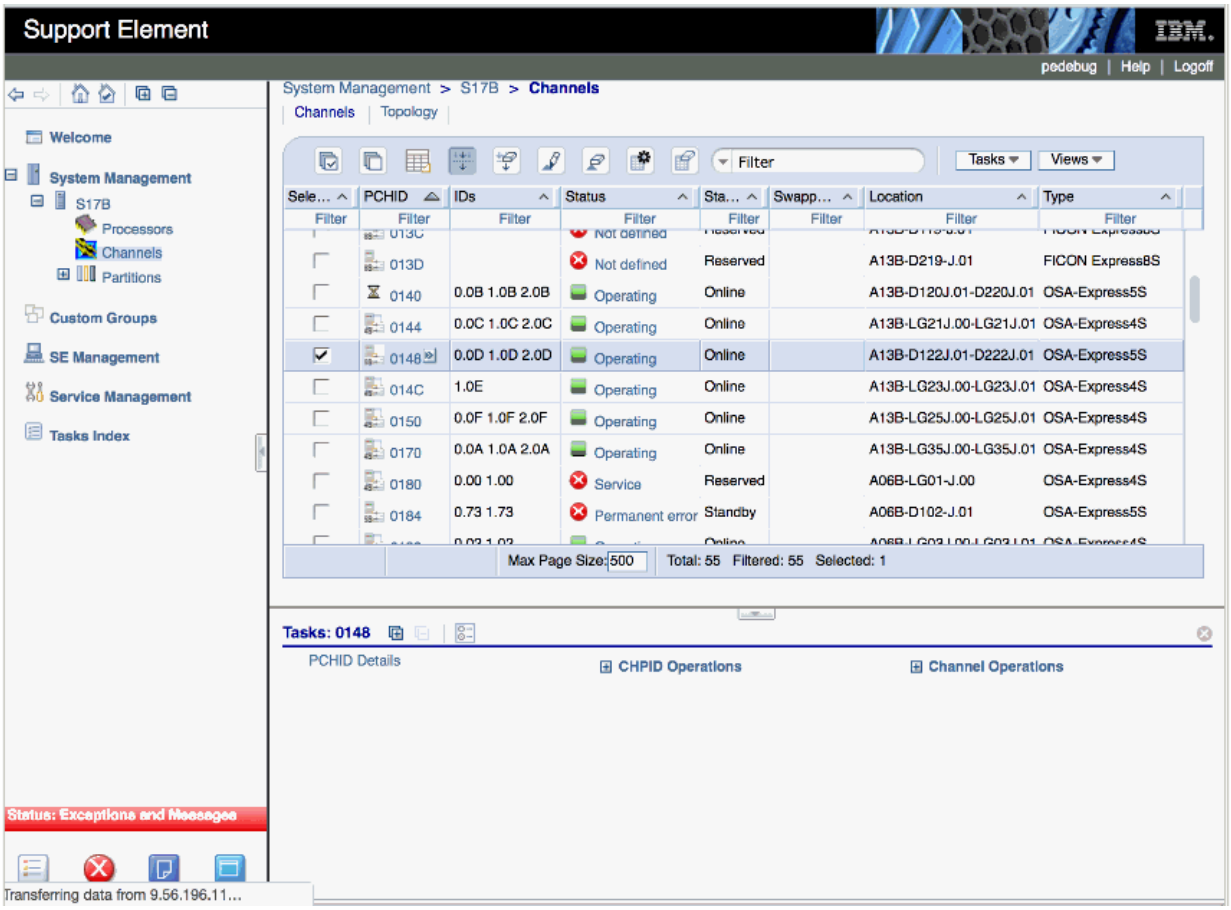
---

4. The ***Standard Channel Advanced Facilities*** window is displayed. Select ***Card Specific Advanced Facilities*** and click OK.

## Accessing the Advanced Facilities window from the SE

### Procedure

1. From the SE workplace window, select the CPC that you want, under **Systems Management** on the left-hand navigation pane.




2. Under the CPC, select **Channels**.
3. From the Channels display, select the PCHID that you want.

# OSA-ICC configuration and debug windows

If it is necessary to bring back the factory defaults, the user can use the “Reset to Defaults” Option of the main window of Advanced Facilities.

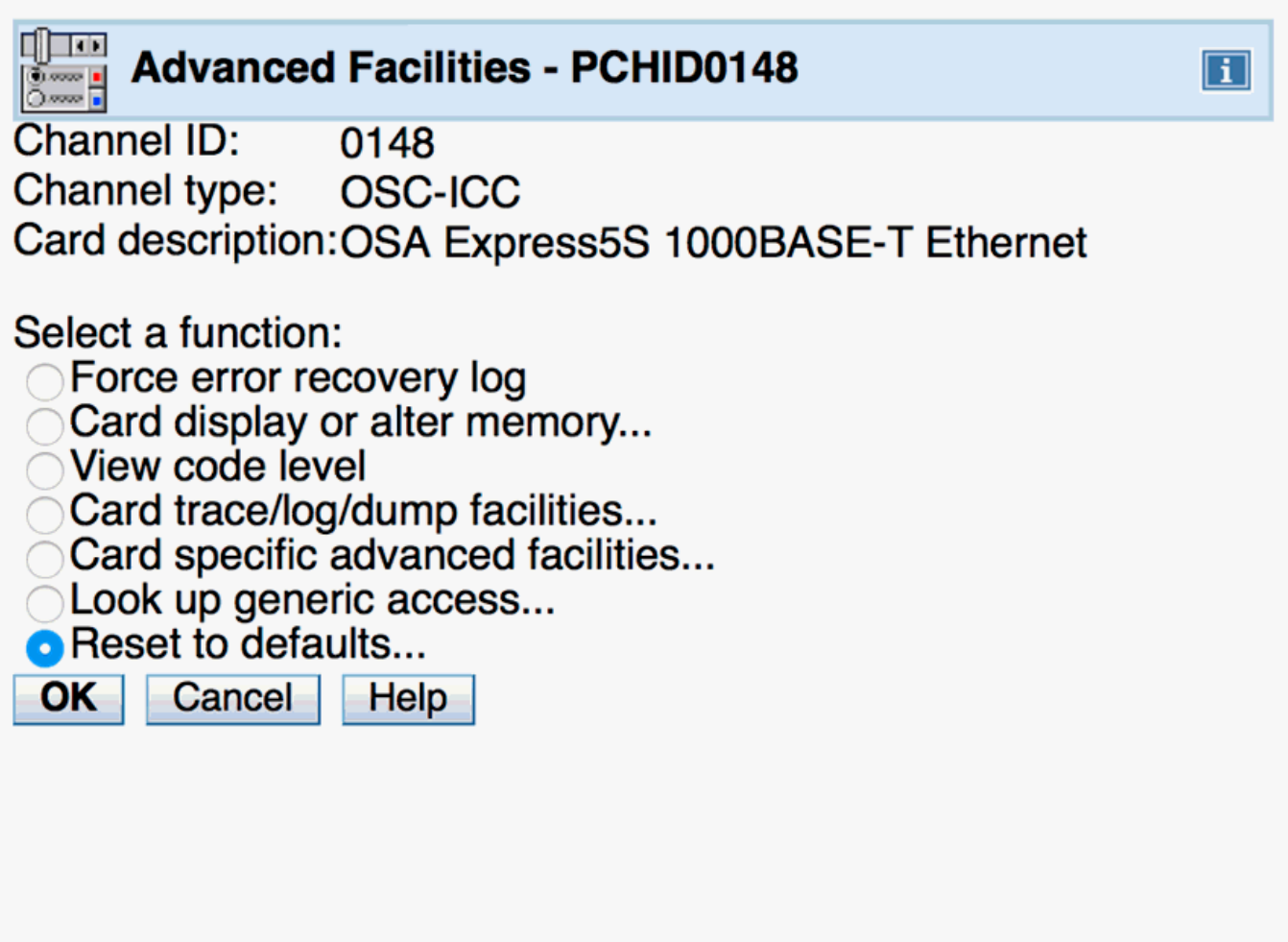



*Figure 5. Reset to defaults*

**Note:** The following functions are not described in this manual:

- Force error recovery
- Card display or alter memory
- View code level
- Card trace/log/dump facilities
- Look up generic access

Management and configuration windows for the ICC are accessed from the Card Specific Advanced Facilities window.

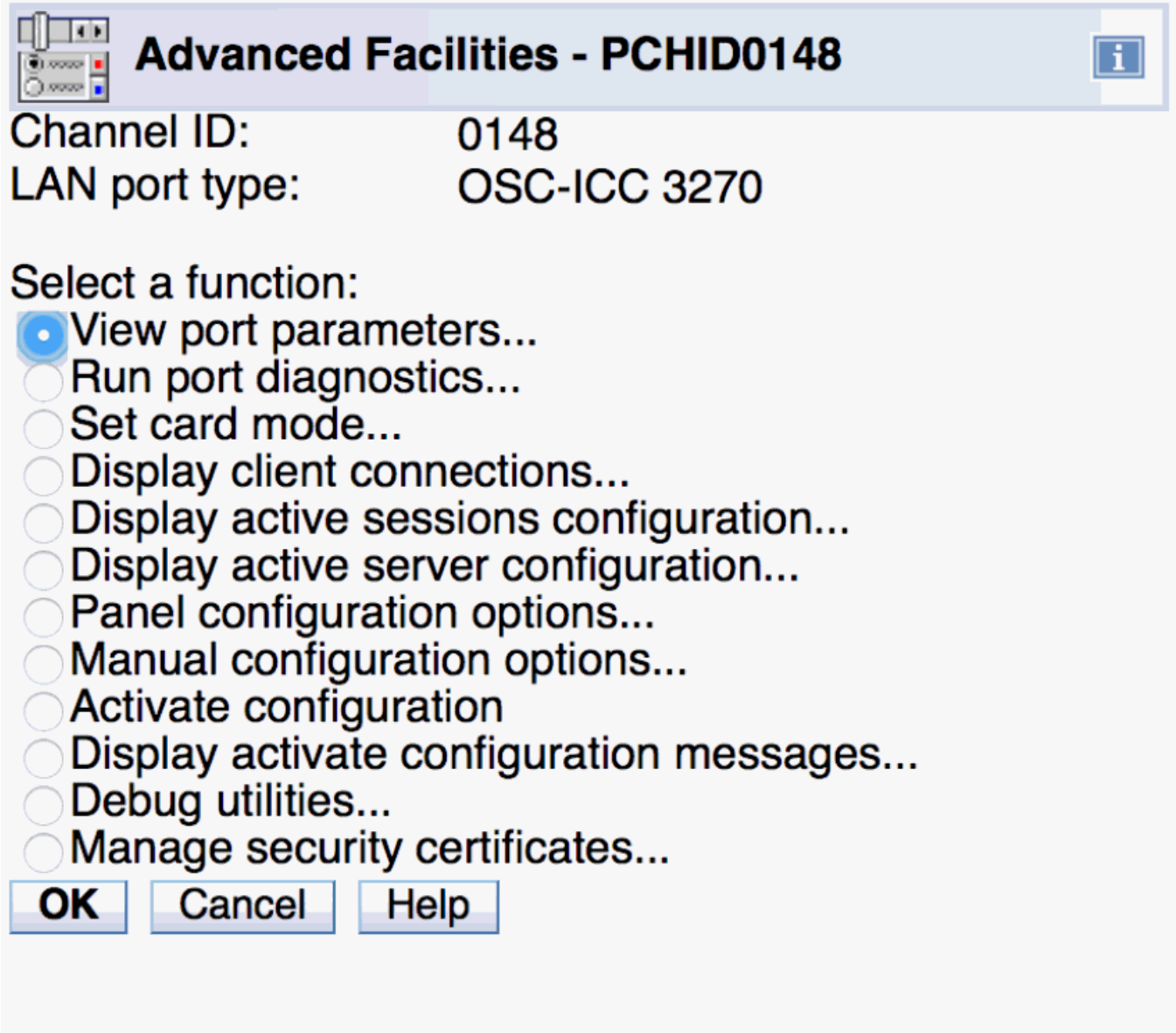



*Figure 6. Card Specific Advanced Facilities window*

All OSA-ICC control operations are selected from the ***Advanced Facilities*** window as shown in "Steps for accessing the Advanced Facilities window" on page 11.

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

| Task | Explanation |
|---|---|
| **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. |

| Task | Explanation |
|---|---|
| **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 windows and the meaning of their entry fields, see "Advanced Facilities windows" on page 16.

## Advanced Facilities windows

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

- View port parameters, see "View port parameters" on page 17
- Run port diagnostics, see "Run port diagnostics" on page 19
- Set card mode, see "Set card mode" on page 21
- Display client connections, see "Display client connections" on page 22
- Display active session configuration, see "Display active session configuration" on page 23
- Display active server configuration, see "Display active server configuration" on page 24
- Panel configuration option, see "Panel configuration options" on page 27
  - Edit session configuration, see "Edit session configuration" on page 30
  - Edit server configuration, see "Edit server configuration" on page 27
  - Validate panel values, see "Validate panel values" on page 33
  - Display validate panel errors, see "Display validate panel errors" on page 34
- Manual configuration options, see Chapter 6, "Manually configuring OSA-ICC," on page 35
  - 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 45
- Activate configuration, see "Activate configuration" on page 46
- Display activate configuration errors, see "Display activate configuration errors" on page 47
- Debug utilities, see Chapter 7, "Debug utilities," on page 49
  - Ping utility, see "Ping Utility" on page 49
  - Trace route utility, see "Trace route utility" on page 51
  - Drop session, see "Drop session" on page 53
  - Logo Control, see "Logo Controls" on page 54
  - Query Command see "Query command" on page 54
- Manage security certificates

## View port parameters

The View port parameters window allows you to view the Network Interface Card statistics. When selected, it gives you statistical and setting information from your OSA-ICC. The port must be active for data to be available. An option is provided to specify the port whose parameters will be displayed.

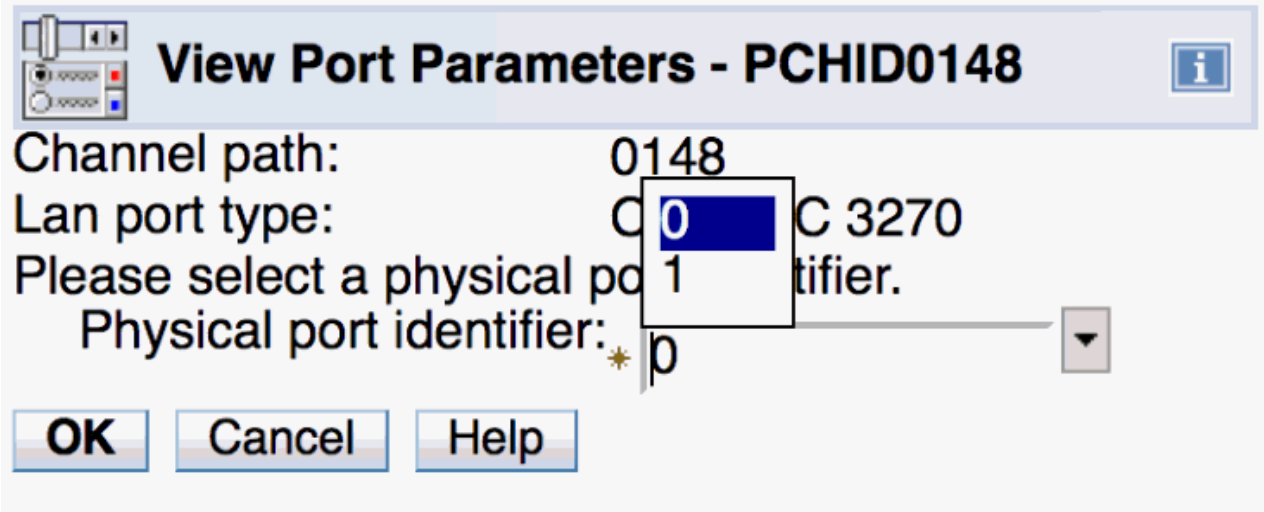



*Figure 7. View port parameters windows (1 of 2)*

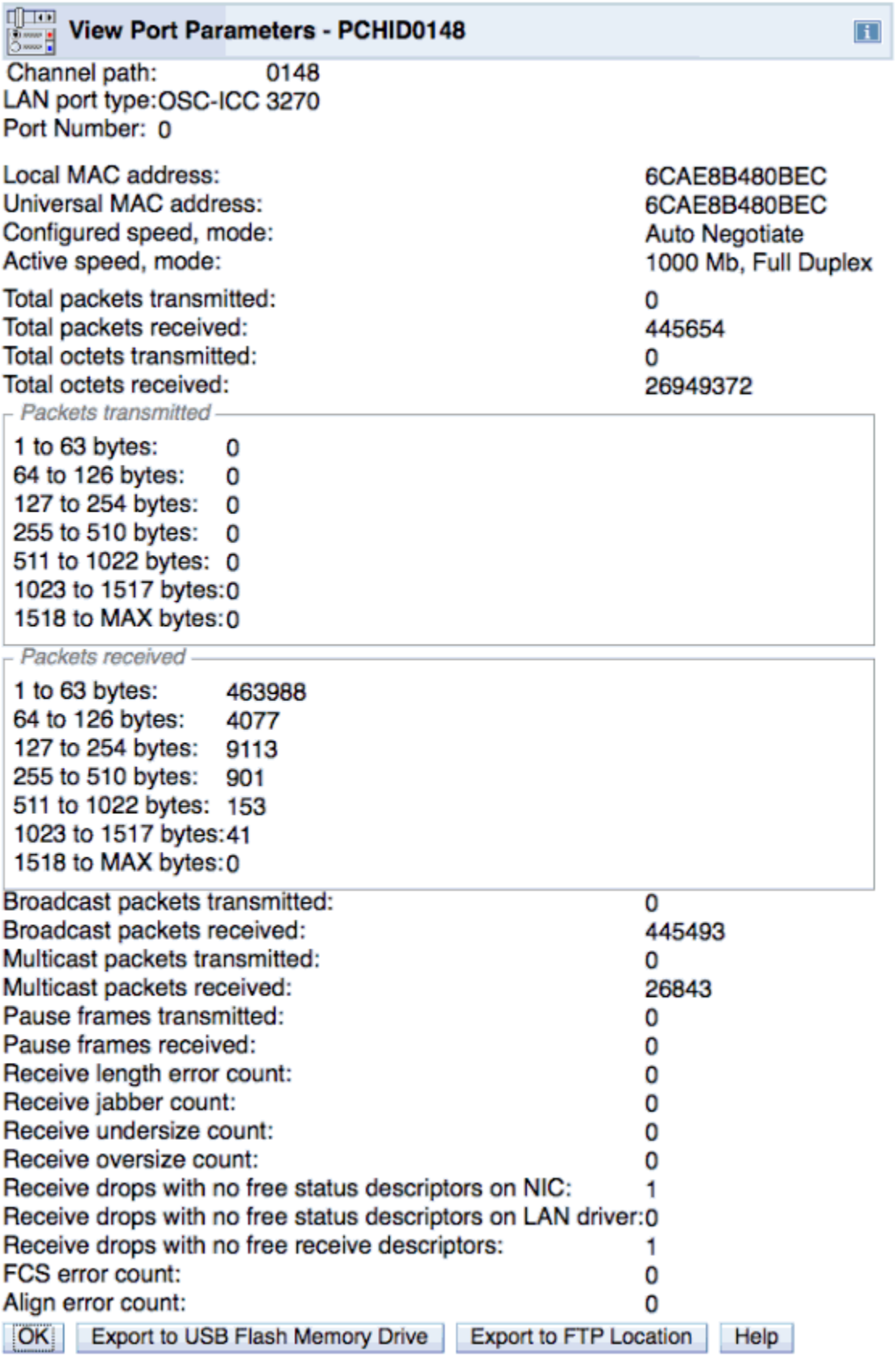



*Figure 8. View port parameters windows (2 of 2)*

The data provided from this window can be Exported to a USB Flash Memory Drive or an external FTP/SFTP Location.

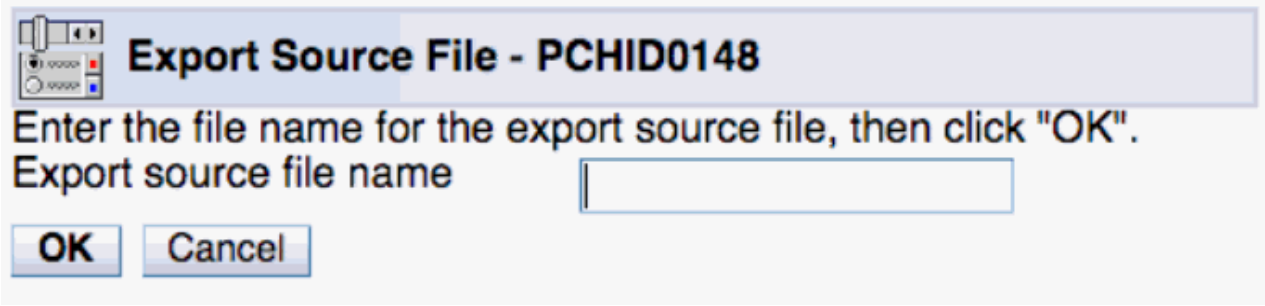



*Figure 9. Export Source File*

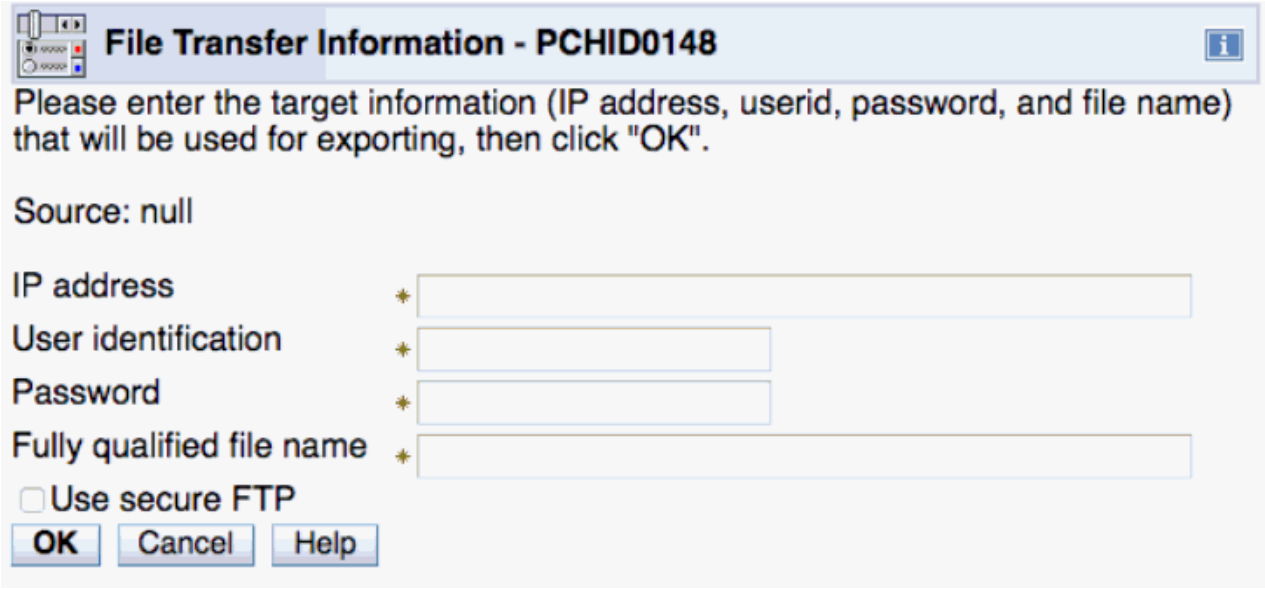



*Figure 10. File Transfer Information*

## Run port diagnostics

The **Run port diagnostics** window is used to run diagnostics. The purpose of running these diagnostics is to verify functionality of the hardware. Running port diagnostics will stop regular traffic on the card and cause all sessions to be disconnected. You can run diagnostics normally or with a wrap plug installed.

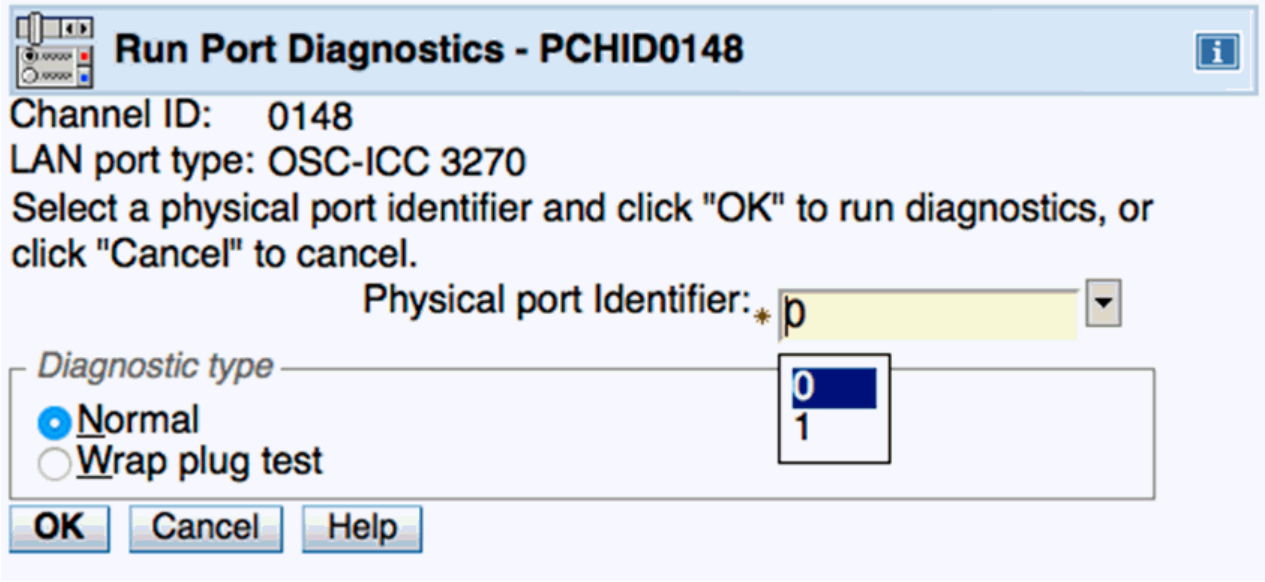



*Figure 11. Run port diagnostics window*

**Port identifier:** Identifies the port on which you want to run diagnostics. The entry field default is 0; however, the desired port can be selected by using the pull down menu.

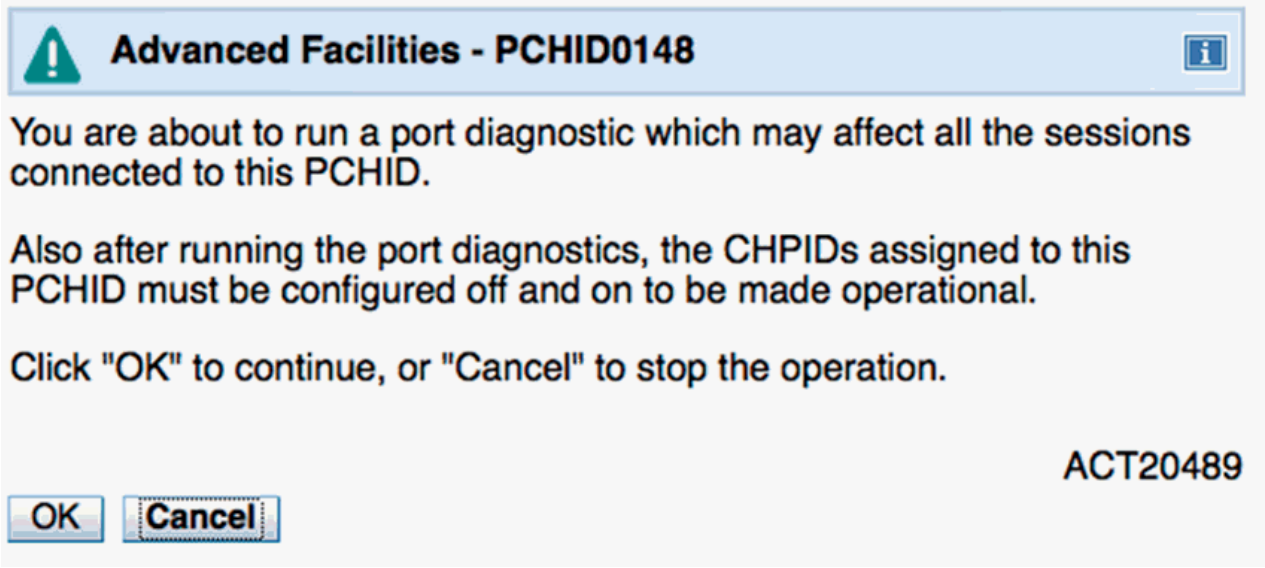



*Figure 12. Port identifier*

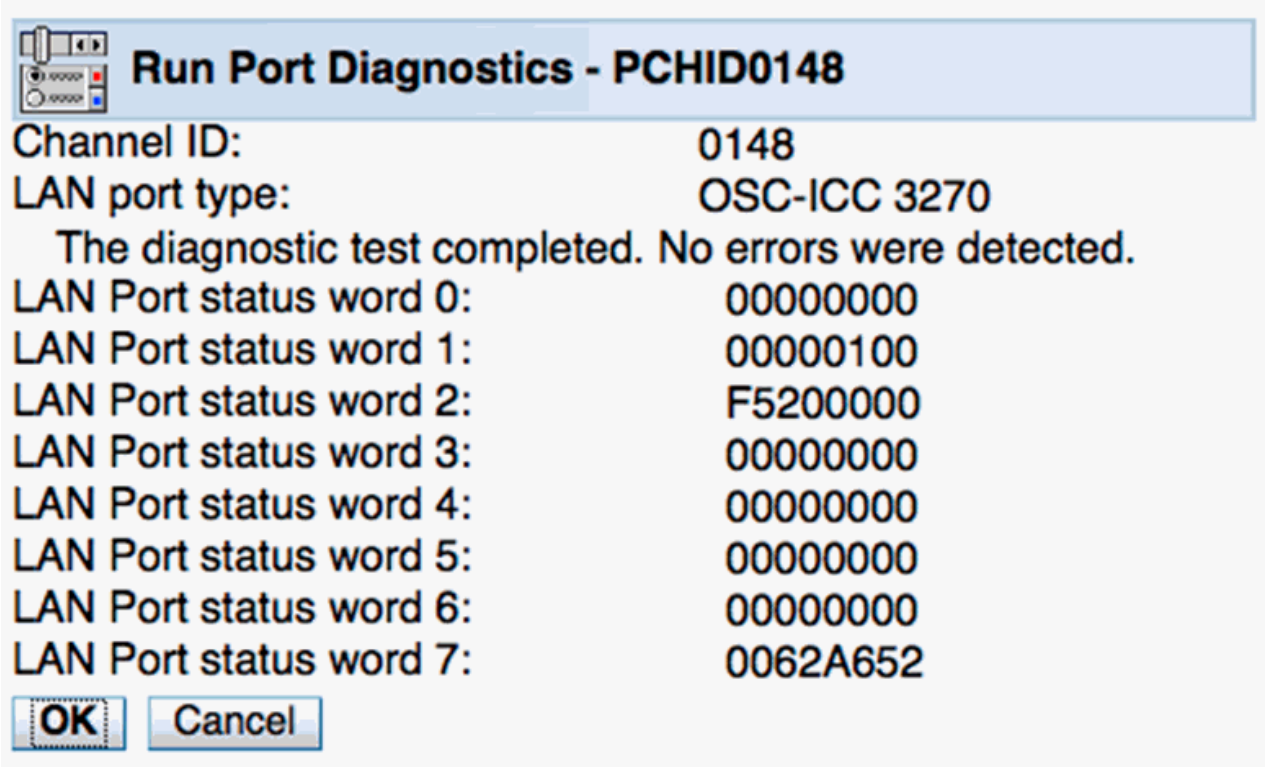



*Figure 13. Run port diagnostics window*

## Set card mode

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

**Note:** This window does not show the current speed or mode of the ICC card. See "View port parameters" on page 17 to see how the card is configured.

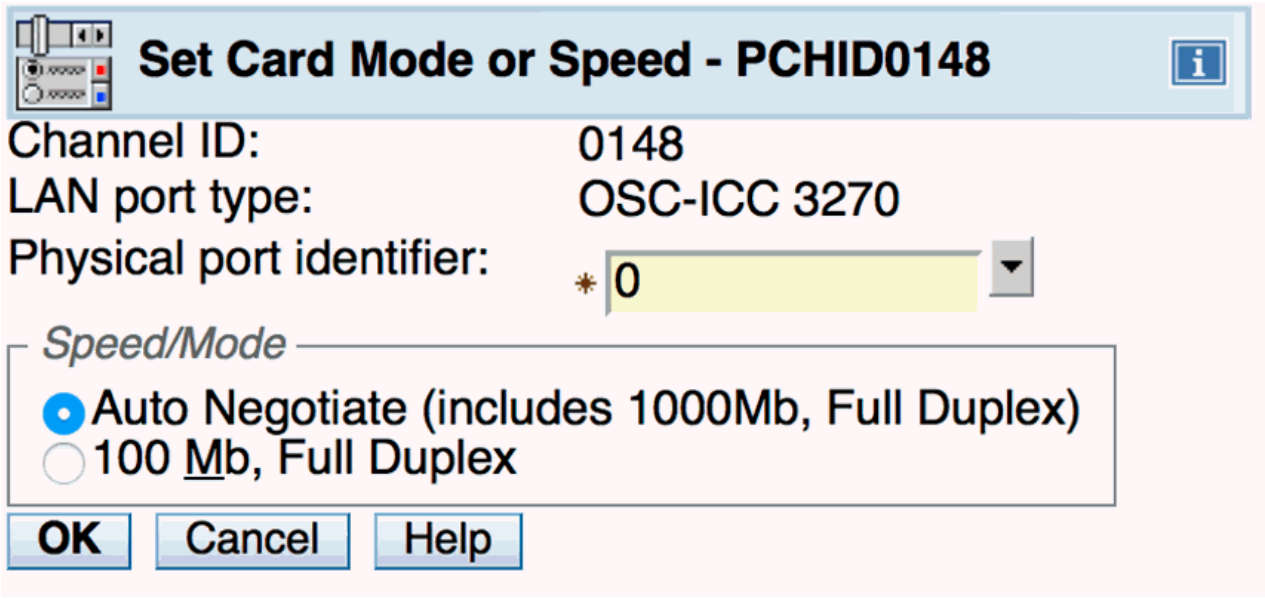



*Figure 14. Set card mode window*

**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, full 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 window. To refresh the information, exit the window and reopen it.

**Display Client Connections - PCHID020C**

Channel ID: 020C

LAN port type: OSA-ICC 3270

| Session Index | Status | Physical Port Identifier | MAC | Client IP | TCP Port | Socket Number | LT Index | Connect Rule | Disable Logo |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Connected | 0 | 52:54:00:F9:55:9E | 10.55.1.84 | 49608 | 134 | 0 | LU Only | No |
| 2 | Connected | 0 | 52:54:00:F9:55:9E | fe80::8d4:d1f2:c8d0:76c6 | 49686 | 135 | 1 | LU Only | No |
| 3 | Connected | 0 | 52:54:00:07:D0:86 | 10.55.1.5 | 60826 | 136 | 2 | LU Only | No |
| 4 | Connected | 0 | 52:54:00:07:D0:86 | 10.55.1.5 | 60828 | 137 | 3 | LU Only | No |
| 5 | Connected | 0 | 52:54:00:07:D0:86 | 10.55.1.5 | 60830 | 138 | 4 | LU Only | No |
| 6 | Connected | 0 | 52:54:00:07:D0:86 | 10.55.1.5 | 60832 | 139 | 5 | LU Only | No |
| 7 | Connected | 0 | 52:54:00:07:D0:86 | 10.55.1.5 | 60834 | 140 | 6 | LU Only | No |
| 8 | Connected | 0 | 52:54:00:07:D0:86 | 10.55.1.5 | 60836 | 141 | 7 | LU Only | No |
| 9 | Connected | 0 | 52:54:00:07:D0:86 | 10.55.1.5 | 60838 | 142 | 8 | LU Only | No |
| 10 | Connected | 0 | 52:54:00:07:D0:86 | 10.55.1.5 | 60840 | 143 | 9 | LU Only | No |
| 11 | Connected | 0 | 52:54:00:07:D0:86 | 10.55.1.5 | 60842 | 144 | 10 | LU Only | No |
| 12 | Connected | 0 | 52:54:00:07:D0:86 | 10.55.1.5 | 60844 | 145 | 11 | LU Only | No |
| 13 | Available | 0 | 00:00:00:00:00:00 | 0.0.0.0 | 0 | 0 | 12 | Unknown | No |
| 14 | Available | 0 | 00:00:00:00:00:00 | 0.0.0.0 | 0 | 0 | 13 | Unknown | No |
| 15 | Available | 0 | 00:00:00:00:00:00 | 0.0.0.0 | 0 | 0 | 14 | Unknown | No |

OK Help

*Figure 15. Display client connections window*

**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 that the client is no longer connected.
- 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.
- TLSConnected : the session is connected via a encrypted TLS enabled session.

**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 same LAN. Otherwise, the MAC address of the router is displayed. This field is not cleared after a client has been disconnected. It represents the last valid MAC address of a successfully connected session.

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

**Port** specifies the TCP port number of the ICC server which the client will connect through. This parameter is only useful to IBM Technical Support.

**Socket Numbers** specifies the Local TCP socket number that uniquely defines the connection. This parameter is only useful to IBM Technical Support.

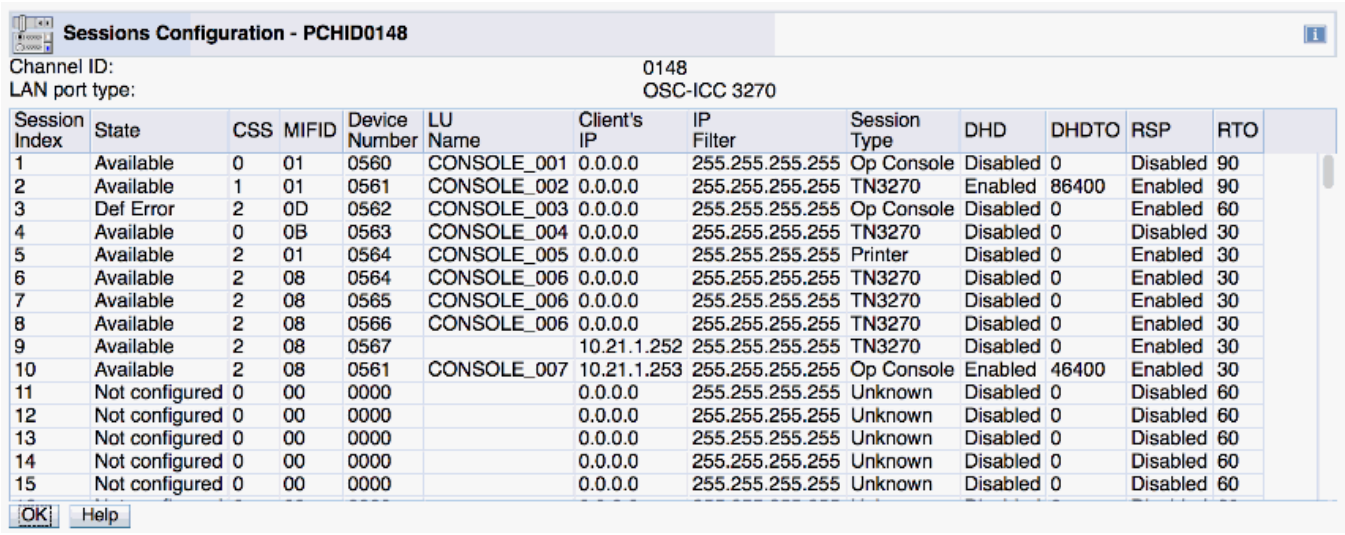
**LT Index** the index in the LT table (OSA-ICC Management table). Valid range is from 0–119. 65535 means initialized. This parameter is only useful to IBM Technical Support.

**Connect rule** can be IP only, LU only, IP & LU, unknown. For more information on connection rules, see Chapter 2, “Server definition rules,” on page 3.

**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*** window 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.




| Session Index | State | CSS | MIFID | Device Number | LU Name | Client's IP | IP Filter | Session Type | DHD | DHDTO | RSP | RTO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Available | 0 | 01 | 0560 | CONSOLE_001 | 0.0.0.0 | 255.255.255.255 | Op Console | Disabled | 0 | Disabled | 90 |
| 2 | Available | 1 | 01 | 0561 | CONSOLE_002 | 0.0.0.0 | 255.255.255.255 | TN3270 | Enabled | 86400 | Enabled | 90 |
| 3 | Def Error | 2 | 0D | 0562 | CONSOLE_003 | 0.0.0.0 | 255.255.255.255 | Op Console | Disabled | 0 | Enabled | 60 |
| 4 | Available | 0 | 0B | 0563 | CONSOLE_004 | 0.0.0.0 | 255.255.255.255 | TN3270 | Disabled | 0 | Disabled | 30 |
| 5 | Available | 2 | 01 | 0564 | CONSOLE_005 | 0.0.0.0 | 255.255.255.255 | Printer | Disabled | 0 | Enabled | 30 |
| 6 | Available | 2 | 08 | 0564 | CONSOLE_006 | 0.0.0.0 | 255.255.255.255 | TN3270 | Disabled | 0 | Enabled | 30 |
| 7 | Available | 2 | 08 | 0565 | CONSOLE_006 | 0.0.0.0 | 255.255.255.255 | TN3270 | Disabled | 0 | Enabled | 30 |
| 8 | Available | 2 | 08 | 0566 | CONSOLE_006 | 0.0.0.0 | 255.255.255.255 | TN3270 | Disabled | 0 | Enabled | 30 |
| 9 | Available | 2 | 08 | 0567 | | 10.21.1.252 | 255.255.255.255 | TN3270 | Disabled | 0 | Enabled | 30 |
| 10 | Available | 2 | 08 | 0561 | CONSOLE_007 | 10.21.1.253 | 255.255.255.255 | Op Console | Enabled | 46400 | Enabled | 30 |
| 11 | Not configured | 0 | 00 | 0000 | | 0.0.0.0 | 255.255.255.255 | Unknown | Disabled | 0 | Disabled | 60 |
| 12 | Not configured | 0 | 00 | 0000 | | 0.0.0.0 | 255.255.255.255 | Unknown | Disabled | 0 | Disabled | 60 |
| 13 | Not configured | 0 | 00 | 0000 | | 0.0.0.0 | 255.255.255.255 | Unknown | Disabled | 0 | Disabled | 60 |
| 14 | Not configured | 0 | 00 | 0000 | | 0.0.0.0 | 255.255.255.255 | Unknown | Disabled | 0 | Disabled | 60 |
| 15 | Not configured | 0 | 00 | 0000 | | 0.0.0.0 | 255.255.255.255 | Unknown | Disabled | 0 | Disabled | 60 |

*Figure 16. Display active session configuration window*

**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 0–5 (depending on machine configuration).

**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. Please refer to connection rules. You can specify a unique LU Name for a connection, or the same LU Name spread across multiple entries. You may also omit this field and connect to a particular host session via the client Host IP.

**Client's IP** (optional) specifies the IP address(es) that the 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. Matching IP addresses are defined by the IP Filter (the next definition).

**IP Filter** defines a range of client IP addresses that are allowed to connect through a given physical port, and is similar to a Subnet Mask. The IP filter is only applicable when the client's IP address is specified.

- Example 1:

  **Client's IP** value is is 10.20.30.40

  **IP Filter** value is 255.255.255.255

  Since all of the bits in the **IP Filter** are on, the IP address of the device that is trying to establish a connection must match the **Client's IP** value exactly. In this example, only 10.20.30.40 will be allowed to connect.

- Example 2:

  **Client's IP** value is 10.20.30.40

  **IP Filter** value is 255.255.255.0

  Since all of the bits in the first three octets of **IP Filter** are on and all of the bits in the last octet of IP Filter are off, the IP address of the device that is trying to establish a connection must match the first three octets of **Client's IP** value exactly, but the last octet can be anything. In this example, devices 10.20.30.0 through 10.20.30.255 would be allowed to connect.

**Session Type** can be TN2370, Op Console (operating system console), or printer

**DHD** (Defer Host Disconnect) indicates whether or not the session is enabled for Deferred Host Disconnect, a function that allows a client to stay virtually connected to the OSA-ICC even though it may be turned off.

**Note:** Each z/OS Master Console input/output console session with the DHD option enabled must have a unique LU name to ensure session auto-reconnection and MSC console recovery occurs correctly. See **LU Name**, described previously in this section.

**DHDTO** (Defer Host Disconnect Time Out): amount of time to wait (in seconds) until OSA-ICC tells the host that the client session has disconnected.

**RSP** (Response Mode): indicates whether telnet response mode is enabled or disabled. If enabled, the host waits for the client emulator to send an telnet acknowledgement for every packet that is transmitted.

| **Note:** |
| --- |
| It is highly recommended that all clients are enabled for Response Mode. |

**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 5-300.

**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), or equivalent on the host operating system, 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.
4. For TLS connected sessions, the recommended value for RTO is 90 seconds.

## Display active server configuration

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

IPv6 protocol support is enabled bringing z14 GA2 code with config off/on or IML. You can configure an IPv4-only, IPv6-only, or both IPv4 and IPv6.

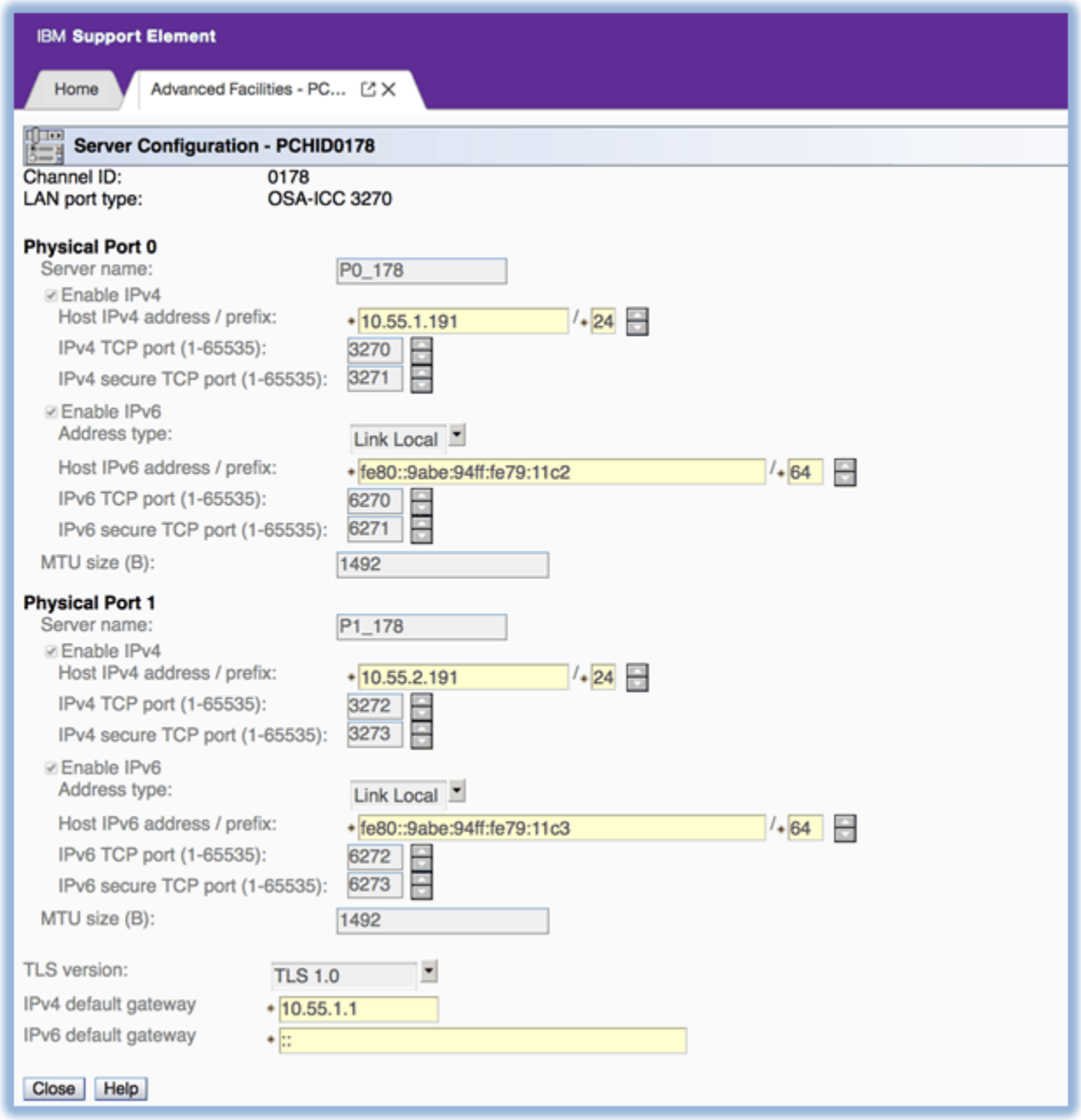



*Figure 17. Display active server configuration window*

For **IPv4** configuration:

**Enable IPv4**
configures the port with an IPv4 address.

**Note:** If this is not selected, the IPv4 configuration is disabled.

**Server Name**
specifies the name of the server to which a client is connected. This name will show up in the 3 line logo that gets sent to all connected clients at the end of a successful telnet negotiation. It is for display only and is not used in tn3270e negotiation or data flow. An example of a 3 line logo is provided in “Logo Controls” on page 54.

**Host IPv4 Address/prefix**
specifies the IP address and prefix associated with this physical port of the OSA-ICC . Prefix to represent the mask in CIDR format.

CIDR notation is a compact representation of an IP address and its associated routing prefix. The notation is constructed from an IP address, a slash ('/'), and a decimal number. The number is the count of leading 1 bits in the subnet mask.

**IPv4 Secure TCP Port**
specifies the port that server will use to connect with the client without encryption. Valid Range is 1-65535. Set to 0 to disable port.

**IPv4 Default Gateway**
specifies IP address gateway to clients that are on a different subnet than the OSA_ICC.

**MTU Size(B)**
specifies the maximum transmission unit (size) to be transferred in one frame. The valid range is from 64–1492 bytes. Refer to your network administrator to determine the maximum frame size your LAN can support.

For **IPv6** configuration:

**Enable IPv6**
configures the port with an IPv6 address.

**Note:** If this is not selected, the IPv6 configuration is disabled.

**Address type**
specifies the address type, either local address IPv6 or static address IPv6.

Link-local: local IPv6 address assigned during network initialization.

Static: user-specified IPv6 address.

**Host IPv6 Address/prefix**
specifies the IP address and prefix associated with this physical port of the OSA-ICC . Prefix to represent the mask in CIDR format.

**Note:** If Address type link local is selected then auto generated link local IPv6 address is assigned and Host IPv6 Address/prefix is grayed out. You cannot edit system generated link local address.

**IPv6 TCP Port**
specifies the port that server will use to connect with the client without encryption. Valid Range is 1-65535. Set to 0 to disable port.

**IPv6 Secure TCP Port**
specifies the port that server will use to connect with the client without encryption. Valid Range is 1-65535. Set to 0 to disable port.

**IPv6 Default Gateway**
specifies IP address gateway to clients that are on a different subnet than the OSA_ICC.

For **TLS** version, the TLS protocol selection feature is enabled through bringing z14 GA2 code config off/on or IML.

TLS protocol VERSION specifies the minimum TLS protocol version to be supported on the PCHID. And it can be selected via drop down box on the Edit Server configuration panel. There is only one TLS protocol version per adapter.

**Note:** By default, TLS version 1.0 is set.

The supported TLS versions are 1.0, 1.1 and 1.2.

If TLS 1.0 is selected, the OSA-ICC 3270 server allows secured client connections for protocols TLS 1.0, TLS 1.1, and TLS 1.2.

If TLS 1.1 is selected, the OSA-ICC 3270 server allows secured client connections for protocols TLS 1.1 and TLS 1.2.

If TLS 1.2 is selected, the OSA-ICC 3270 server allowx secured client connections for protocol TLS 1.2.

# Chapter 5. Configuring OSA-ICC

Configuring your OSA-ICC results in the creation of a configuration file containing session and server configuration information on the SE disk. You can create or modify this file by entering data into the fields of Panel Configuration Options Task or by using a text editor to manually add or delete entries into the file directly. Panel entry requires that you move through a series of data entry panels and enter configuration data and complete the required fields. 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 via the panel or manual entry methods, either interface can be used to update the file.

**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 45 and "Activate configuration" on page 46. 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.

| **Important note:** |
| --- |
| The OSA-ICC configuration file is generated every time the user configures the pchid on/off or enters Advanced facilities. Therefore, partial editing sessions are not allowed. To save a configuration to an OSA-ICC card, you must validate/activate the configuration. If you wish to save a partially edited configuration file, the user should export the source file via USB or ftp in the Manual Configurations Options window. |

| **Important note:** |
| --- |
| If you try to activate a configuration that has validation errors in it, the configuration file will be returned to the last good configuration. Validation Warnings are allowed (return code < 1000 are considered warnings). Configurations with warnings can be successfully activated. |

## Panel configuration options

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

### Edit server configuration

The ***Edit server configuration*** window is used to edit the server configuration for a given OSC.

- If a 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 enabled. Setting a Port number (whether it is the Secure or non-Secure Port) to 0 will disable that connection port type for that OSA-ICC Server IP Address. Figure 18 on page 28 shows Port 1 disabling Secure Connections to it.

**Note:** To enable only Secure connections to an OSA-ICC Server, set the TCP Port fields in each Physical Port Definition Section to 0. This will disable all non-secure traffic to this OSA-ICC IP Address.

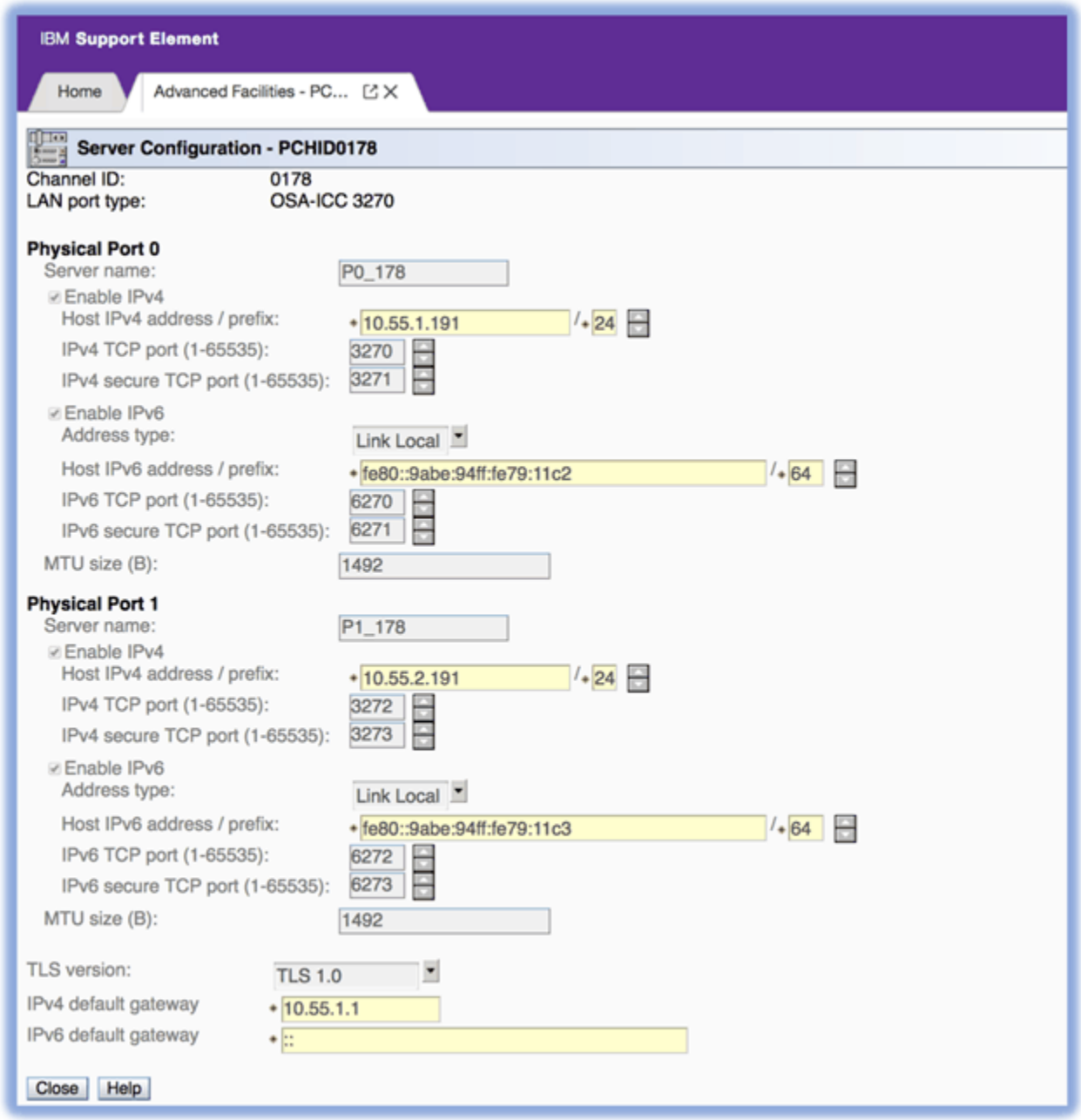



*Figure 18. Edit server configuration window*

The Edit server configuration window is used to edit the server configuration for a given OSC.

IPv6 protocol support is enabled bringing z14 GA2 code with config off/on or IML.

1. You can configure an IPv4-only, IPv6-only, or both IPv4 and IPv6.
2. If both the check boxes (Enable IPv4 and Enable IPv6) are not selected then the given port is disabled
3. At least one port must be defined at a given time in order for the server to be enabled. Setting a Port number (whether it is the Secure or non-Secure Port) to 0 will disable that connection port type for that OSA-ICC Server IP Address. Figure 18 on page 28 shows Port 1 disabling Secure Connections to it.
4. Use this drop down box to select the minimum TLS protocol version(1.0 or 1.1 or 1.2) to be supported on the PCHID.

   **Note:** By default, TLS version 1.0 is set.

**Note:** To enable only Secure connections to an OSA-ICC Server, set the TCP Port fields in each Physical Port Definition Section to 0. This will disable all non-secure traffic to this OSA-ICC IP Address.

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

For **IPv4** configuration:

**Enable IPv4**
configures the port with an IPv4 address.

**Note:** If this is not selected, the IPv4 configuration is disabled.

**Server Name**
specifies the name of the server to which a client is connected. This name will show up in the 3 line logo that gets sent to all connected clients at the end of a successful telnet negotiation. It is for display only and is not used in tn3270e negotiation or data flow. An example of a 3-line logo is provided in "Logo Controls" on page 54.

**Host IPv4 Address/prefix**
specifies the IP address and prefix associated with this physical port of the OSA-ICC . Prefix to represent the mask in CIDR format.

CIDR notation is a compact representation of an IP address and its associated routing prefix. The notation is constructed from an IP address, a slash ('/'), and a decimal number. The number is the count of leading 1 bits in the subnet mask.

**IPv4 Secure TCP Port**
specifies the port that server will use to connect with the client without encryption. Valid Range is 1-65535. Set to 0 to disable port.

**IPv4 Default Gateway**
specifies IP address gateway to clients that are on a different subnet than the OSA_ICC.

**MTU Size(B)**
specifies the maximum transmission unit (size) to be transferred in one frame. The valid range is from 64–1492 bytes. Refer to your network administrator to determine the maximum frame size your LAN can support.

**Note:** This field is applicable to both IPv4 and IPv6 connections.

For **IPv6** configuration:

**Enable IPv6**
configures the port with an IPv6 address.

**Note:** If this is not selected, the IPv6 configuration is disabled.

**Address type**
specifies the address type, either local address IPv6 or static address IPv6.

Link-local: local IPv6 address assigned during network initialization.

Static: user-specified IPv6 address.

**Host IPv6 Address/prefix**
specifies the IP address and prefix associated with this physical port of the OSA-ICC . Prefix to represent the mask in CIDR format.

**Note:** If Address type link local is selected then auto generated link local IPv6 address is assigned and Host IPv6 Address/prefix is grayed out. You cannot edit system generated link local address.

**IPv6 TCP Port**
specifies the port that server will use to connect with the client without encryption. Valid Range is 1-65535. Set to 0 to disable port.

**IPv6 Secure TCP Port**
specifies the port that server will use to connect with the client without encryption. Valid Range is 1-65535. Set to 0 to disable port.

**IPv6 Default Gateway**
specifies IP address gateway to clients that are on a different subnet than the OSA_ICC.

For **TLS** version, the TLS protocol selection feature is enabled through bringing z14 GA2 code config off/on or IML.

1. Use the drop down box to select the minimum TLS protocol version(1.0 or 1.1 or 1.2) to be supported on the PCHID

   **Note:** By default, TLS version 1.0 is set.
2. Downgrading the protocol version **does not terminate** the SSL sessions that are active on higher protocol version. That is,
   - Have sessions connected at protocol version 1.2
   - Edit the server config panel and change the protocol version to 1.1
   - Validate and activate
   - Upon activate, sessions connected with protocol 1.2 will not be terminated.
3. Upgrading the protocol version **does not terminate** the SSL sessions that are active on lower protocol version. That is,
   - Have sessions connected at protocol version 1.0
   - Edit the server config panel and change the protocol version to 1.1
   - Validate and activate
   - Upon activate, sessions connected with protocol 1.0 will not be terminated.

**Note:** The recommended value for MTU is 1492.

## Edit session configuration

The ***Edit session configuration*** window 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. To open the **Edit session configuration** window, select Edit sessions configuration from the **Panel configuration options** window:

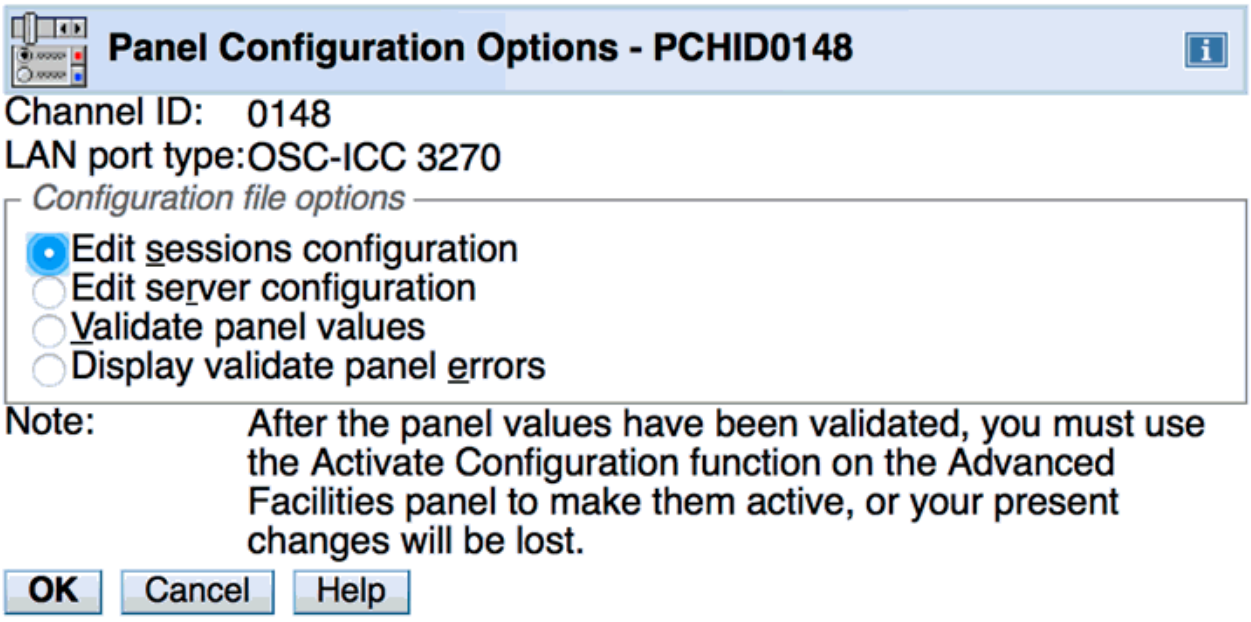



*Figure 19. Panel configuration options window*

The following is the **Edit session configuration** window:

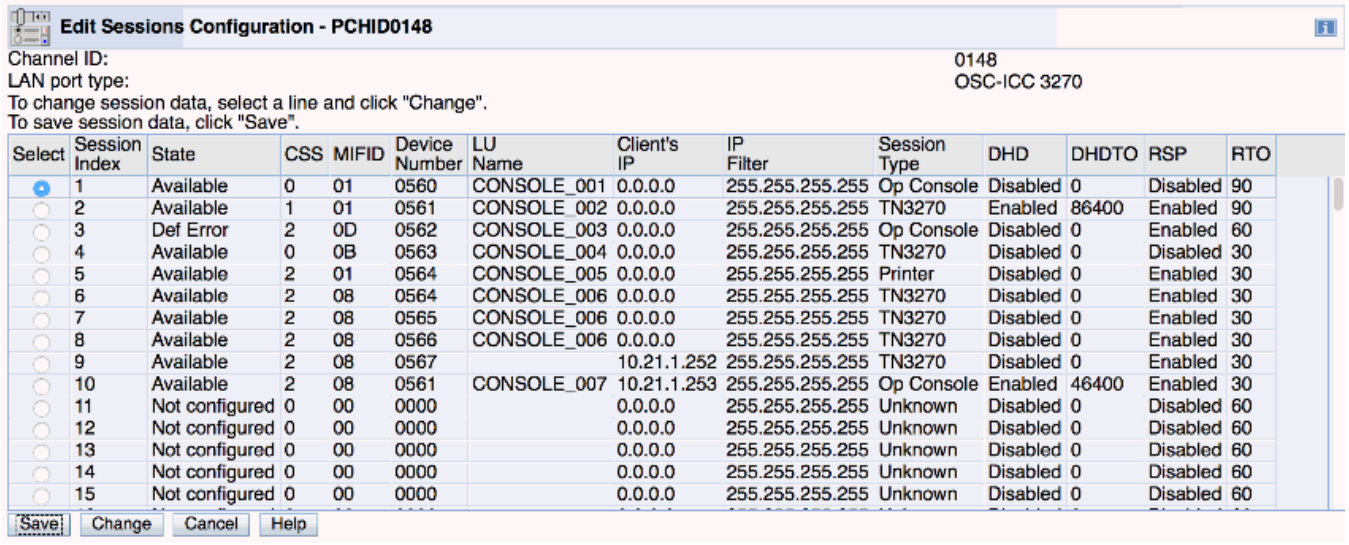



*Figure 20. Edit session configuration window*

To edit a field:

1. Select the radio button for the entry you want to edit
2. Click the change button at the bottom of the window
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 below.
4. Click OK to save the updated session information or the information will be lost.
5. Click Save on the Edit Session Configuration window or the information will be lost.
6. Validate and activate your changes. For more information on validating and activating see “Validate panel values” on page 33 and “Activate configuration” on page 46. In addition, you may want to export your configuration as backup. For more information on exporting, see “Export source file” on page 37.

**Important Note**: If you try to activate a configuration that has validation errors in it, the configuration file will be returned to the last good configuration. Validation Warnings are allowed (return code < 1000 are considered warnings). Configurations with warnings can be successfully activated.

**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 0–5.

**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 that was defined in the IOCDS.

**LU Name** defines a group or pool of devices which identifies what session you are going to connect to. See “Client connection rules” on page 3 for more information. You can specify a unique LU Name for a connection, or the same LU Name spread across multiple entries. You may also omit this field and connect to a particular host session via the client's IP address.

**Client's IP** (optional) specifies the IP address that a 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 will be 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 TN2370, Op Console (operating system console), or printer.

**DHD** (Defer Host Disconnect): indicates whether or not the session is enabled for Deferred Host Disconnect (a function that allows a client to stay virtually connected to the OSA-ICC even though it may be turned off).

1. Disable

   Immediately notify host OS of a disconnect

   After reconnecting, a manual Vary on-line (at an alt zOS Ops Console) must be performed to reconnect the Session.
2. Enable with defaulted deferment of 60 seconds

   Wait for 60 seconds before notifying host OS

   - If reconnected within 60 seconds, simulate a "3270 Clear key"
   - z/OS MCS console support will reformat the screen and continue
3. Enable with no timeout for deferment

   Never notify the host OS (will leave in disconnected state)
4. Enable with user specified defaulted deferment

   The same as item 2 in this list, with a different time value

**DHDTO** (Defer Host Disconnect Time Out): amount of time to wait (in seconds) until OSA-ICC tells the host that the client session has disconnected.

**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.

| **Note:** |
| --- |
| It is highly recommended that all clients are enabled for Response Mode. |

**RTO** (Response Time Out) specifies how long to wait (in seconds) for a response from the client before performing a client disconnect. The valid range for RTO is 5-300.

**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.
3. For TLS connected sessions, the recommended value for RTO is 90 seconds.
4. The default RTO is 60 seconds.

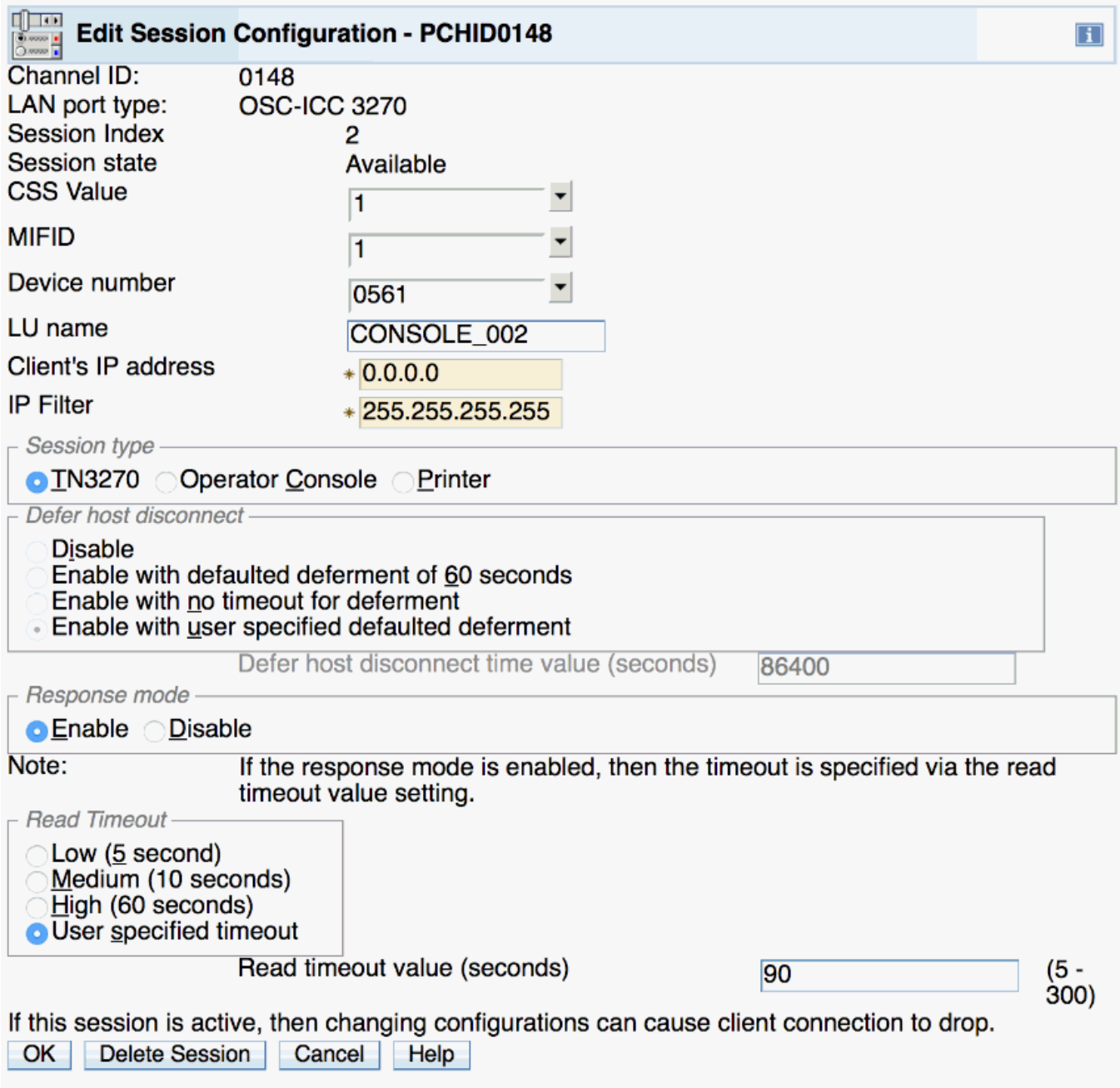



*Figure 21. Edit session configuration window*

To remove a session definition, click Delete Session on the bottom of the window.

## Validate panel values

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

**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 46. 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 11, "Error and warning messages," on page 91.

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.

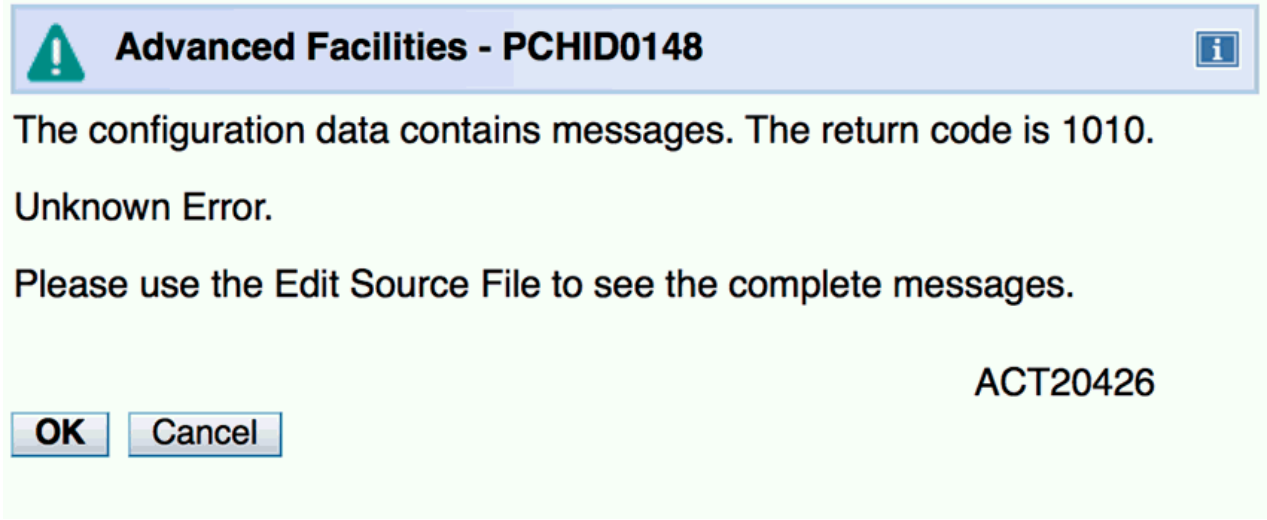



*Figure 22. Validate panel values window*

## Display validate panel errors

The ***Display validate panel errors*** window 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 11, “Error and warning messages,” on page 91.

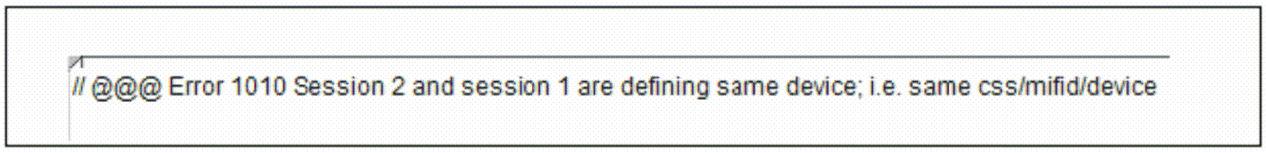



*Figure 23. Display validate panel errors window*

Other Examples of Error and Warning Messages :

```
// @@@ Error 1126: This Session # has already been configured
// @@@ warning: This session is in Definition Error state
```

# Chapter 6. Manually configuring OSA-ICC

Configuring your OSA-ICC results in the creation of a session configuration file on the SE disk. You can create this file by entering data via window entry or by manually editing the file. The window entry requires that you move through a series of data entry windows and enter configuration data in those windows. Your other option is to edit your configuration manually using your favorite workstation editor. Manual editing is faster for changing multiple data entries because of the 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 via FTP or to a USB or other supported device, edit it using the editor 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*** window under the ***Manual configurations options*** window.

**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 45 and "Activate configuration" on page 46. 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.

| **Important note:** |
| --- |
| The OSA-ICC configuration file is generated every time the user configures the pchid on/off or enters Advanced facilities. Therefore partial editing sessions are not allowed. To save a configuration to an OSA-ICC card, you must validate/activate the configuration. If you wish to save a partially edited configuration file, the user should export the source file via USB or ftp in the Manual Configurations Options window. |

| **Important note:** |
| --- |
| If you try to activate a configuration that has validation errors in it, the configuration file will be returned to the last good configuration. Validation Warnings are allowed (return code < 1000 are considered warnings). Configurations with warnings can be successfully activated. |

**Important Note**: If you try to activate a configuration that has validation errors in it, the configuration file will be returned to the last good configuration. Validation Warnings are allowed (return code < 1000 are considered warnings). Configurations with warnings can be successfully activated.

## Manual configurations options

The ***Manual configurations options*** window is the high level selection window 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.

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

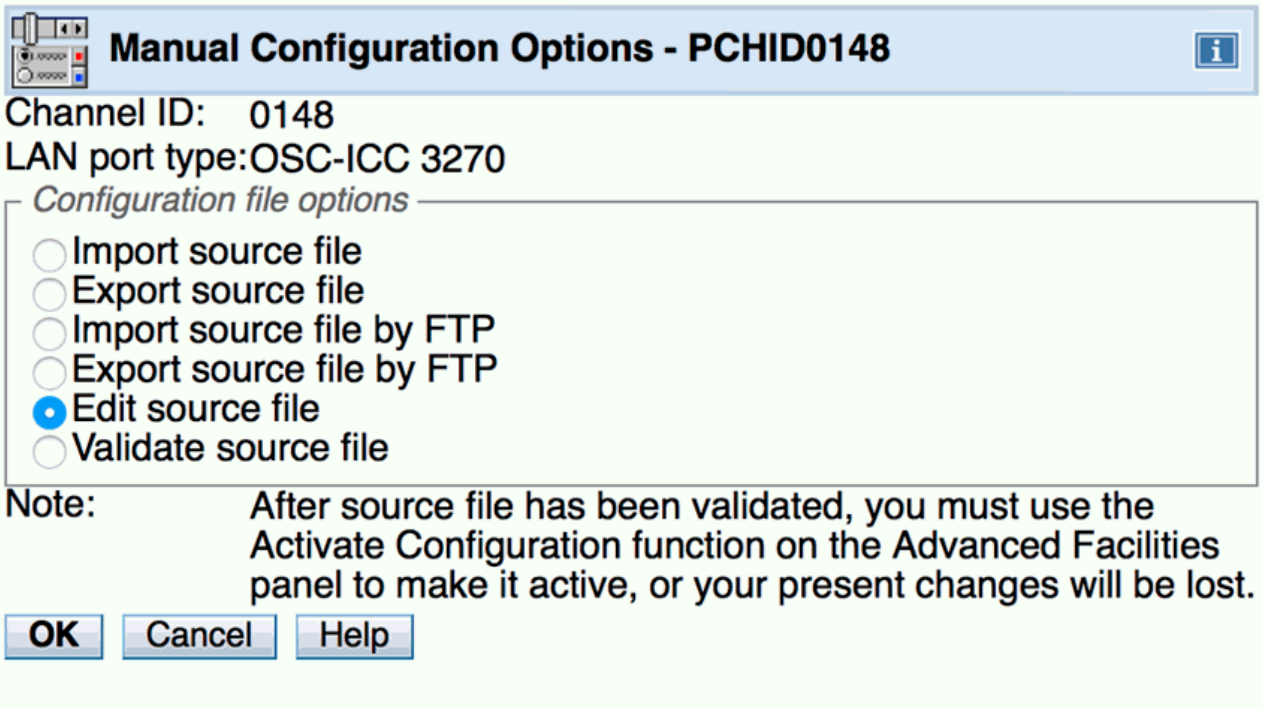



*Figure 24. Manual configuration window*

## Import source file

If you have previously saved a copy of a OSA-ICC configuration, it must be imported before the changes can be applied.

### 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 device into SE or HMC. 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 or other supported device in the SE.
2. From the ***Manual configuration options*** window select ***Import source file***. The ***Import source file*** window appears with a list of all the files on the disk.

   **For example:**

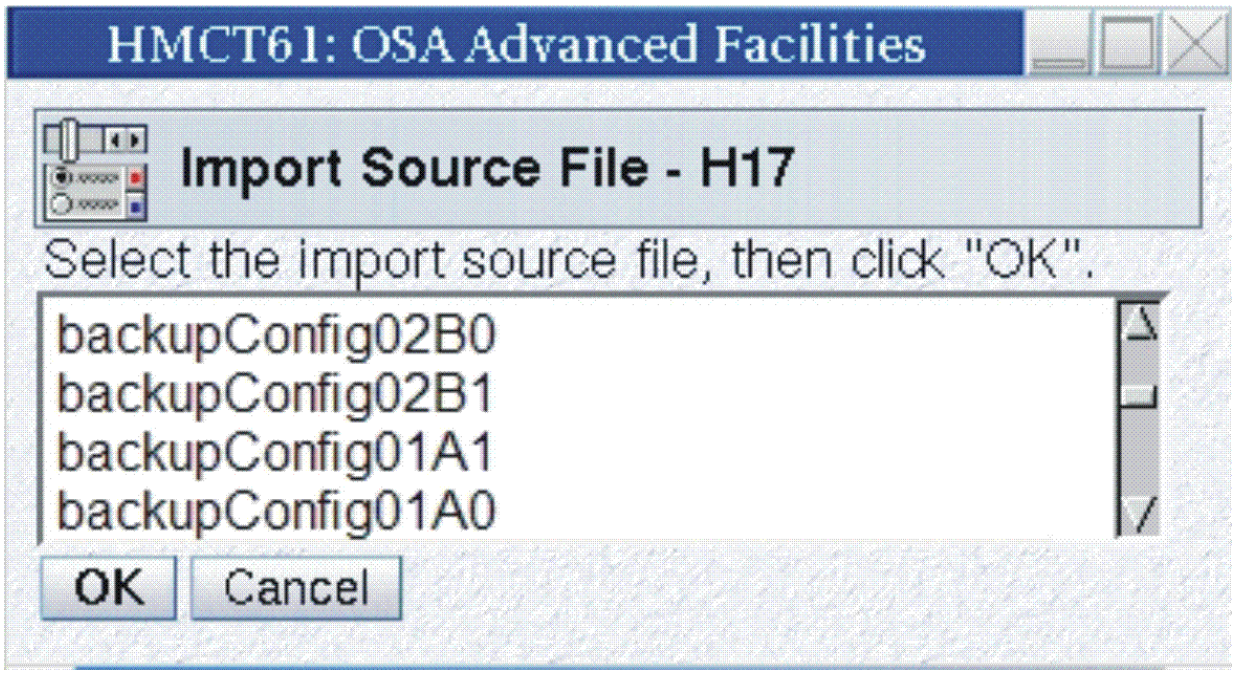



*Figure 25. Import source file window*

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

   **Note:** The OSA-ICC can only import one file at a time. Subsequent imports will overwrite the present configuration you are working on even if the remote file has a different name.

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

## Export source file

The ***Export source file*** window is used to export a session configuration file to a USB or other supported device so you can save your configurations or edit the configuration file with your editor.

### 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 export will be from the SE. If you are working from the Hardware Management Console, the export will be from the Hardware Management Console. If your Hardware Management Console is in single object operation, you must insert the USB or other supported device in the SE.
2. From the ***Manual configuration options*** window select ***Export source file***. The ***Export source file*** will appear.

   **For example:**

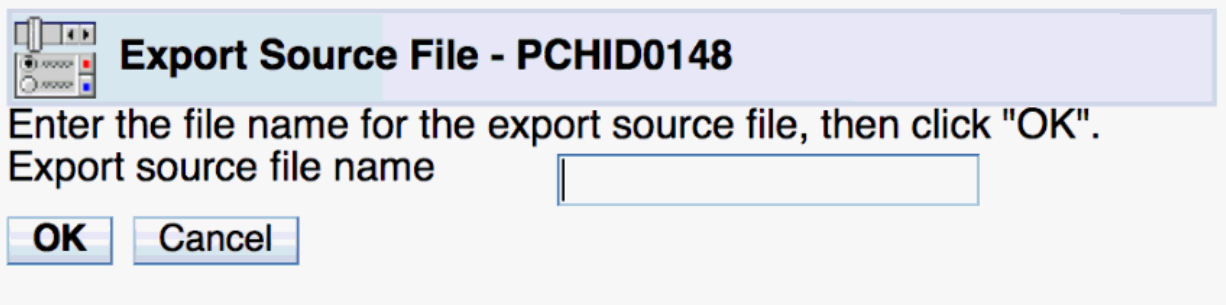



*Figure 26. Export source file window*

3. Type in the name to be given to the exported configuration file in the Export source file name field and click OK.

## Import source file via FTP

If you exported a configuration file for editing you must import it in order to use it.

**Steps for importing a configuration file via FTP or SFTP**

**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*** window select ***Import source file via FTP***. The ***Import source file via FTP*** will appear.

   **For example:**

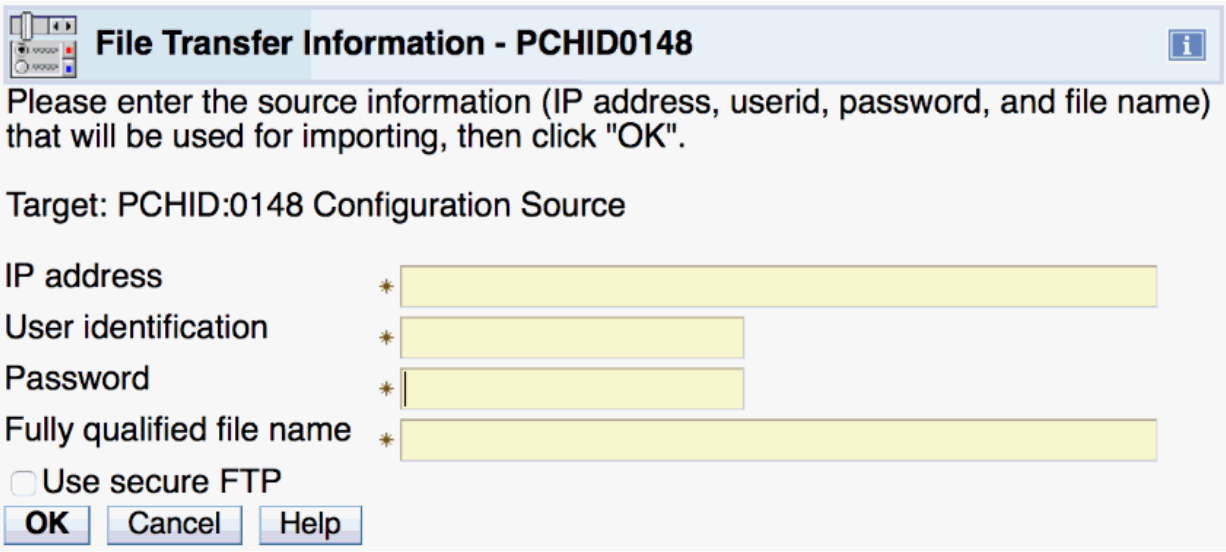



*Figure 27. Import source file via FTP window*

2. Enter the IP address, user identification, password, and fully qualified file name and click OK. The file you specified will be imported. You can choose to import your file securely by clicking the Use secure FTP option on the transfer window.

   **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 with warning" 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.

### 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*** window select ***Export source file via FTP***. The ***Export source file via FTP*** will appear.

   **For example:**

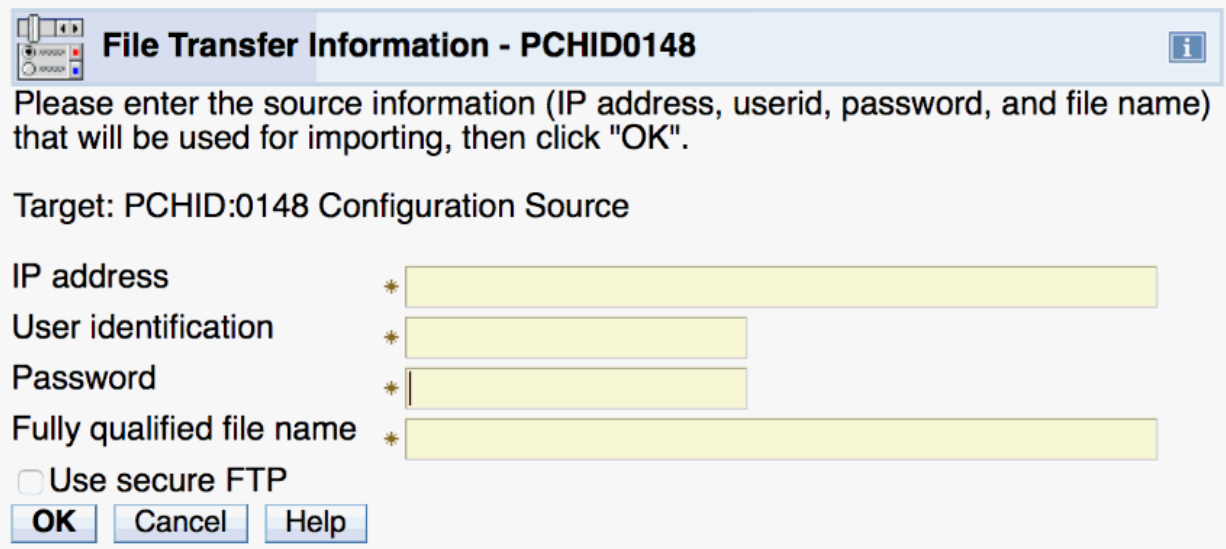



   *Figure 28. Export source file via FTP window*

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. You can choose to import your file securely by clicking the Use secure FTP option on the transfer window.

## 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*** window.

**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 window), 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 45 and "Activate configuration" on page 46.

### Steps for editing a source file

1. From the ***OSC manual configuration*** window 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 with warning" on page 40.
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 an error" on page 42.

## Sections of the configuration file

There are three sections contained in the configuration file – only two of which are necessary for configuration.

1. The first Section is an informational comment section. All comments are proceeded with the // symbol. This section provides status on what time and version of code was used to generate the configuration file. The user is not required to add these comments to configuration files they generate themselves. It is purely informational. Typical information that could be provided (subject to change) is as follows:

```
// This file has been generated from the binary file /console/data/iqzc0148.hut
// by the SE ICC Java Code on 2016.02.26-19:09:05
// Java Code Level= 605 OSA Code Version= 0
// Certificate Activate Time 2016.02.26-19:09:03
// Certificate Create Time (only full if this chpid created Certs)  N/A
// Certificate Files Date created on SE2016.02.19-13:03:52
```

2. The second section is called the Server Configuration section and includes parameters about the OSC Server definitions. Tags are used in the file, to delineate certain information relating to the configuration. In the file, the first line of the server section must be **<OSC_SERVER>** and the last line of the server section must be **</OSC_SERVER>**.

   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.

3. The third section of the configuration file includes parameters about the TN3270E sessions you want to configure on your OSA-ICC. You can configure up to 120 sessions on an OSA-ICC.

   **Note:** Only 48 of these sessions can be active on a Secure TCP port connection at one time.

The first line of the session section must be **<CONFIG_SESSION>** and the last line must be **</CONFIG_SESSION>**.

Within the **<CONFIG_SESSION>** section of the file are the individual session configuration parameters. Each set of 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.

### Example of a correct configuration file with warning

The following is an example of a configuration file. This example matches the window and Manual Configuration window examples given throughout the document

```
// This file has been generated from the binary file /console/data/iqzc0148.hut
// by the SE ICC Java Code on 2016.02.26-19:09:05
// Java Code Level= 605 OSA Code Version= 0
// Certificate Activate Time 2016.02.26-19:09:03
// Certificate Create Time (only full if this chpid created Certs) N/A
// Certificate Files Date created on SE2016.02.19-13:03:52

<OSC_SERVER>
<OSC_PHYSICAL_PORT0>
  HOST_IP= 10.55.1.190
  SUBNET_MASK= 255.255.255.0
  PORT= 3270
  SECURE_PORT= 3271
  HOST_LL_ADDRESS/PREFIX=  fe80::9abe:94ff:fe79:14dc/64
  ADDR_TYPE= LINK_LOCAL
  HOST_IPV6_ADDRESS/PREFIX=  fe80::9abe:94ff:fe79:14dc/64
  IPV6_PORT= 6270
  IPV6_SECURE_PORT= 6271
  ETHERNET_FRAME= DIX
  MTU= 1492
  NAME= 17C_0
</OSC_PHYSICAL_PORT0>

<OSC_PHYSICAL_PORT1>
  HOST_IP= 10.55.2.190
  SUBNET_MASK= 255.255.255.0
  PORT= 3272
```

```
  SECURE_PORT= 3273
  HOST_LL_ADDRESS/PREFIX=  fe80::9abe:94ff:fe79:14dd/64
  ADDR_TYPE= LINK_LOCAL
  HOST_IPV6_ADDRESS/PREFIX=  fe80::9abe:94ff:fe79:14dd/64
  IPV6_PORT= 6272
  IPV6_SECURE_PORT= 6273
  ETHERNET_FRAME= DIX
  MTU= 1492
  NAME= 17C_1
</OSC_PHYSICAL_PORT1>

TLS_VERSION= 1.0
DEFAULT_GATEWAY= 10.55.1.1
IPV6_DEFAULT_GATEWAY=  2::1

</OSC_SERVER>
<CONFIG_SESSION>
<SESSION1>
CSS= 00 IID= 01 DEVICE= 0560 GROUP= "CONSOLE_001"
CONSOLE_TYPE= 2 RESPONSE= OFF  READ_TIMEOUT= 90
</SESSION1>

<SESSION2>
// @@@ warning: This session is in Definition Error
//              state CSS= 01 IID= 01 DEVICE= 0a60
GROUP= "CONSOLE_002"
CONSOLE_TYPE= 1 RESPONSE= ON READ_TIMEOUT= 90
DEFER_HOST_DISCONNECT= 86400
</SESSION2>

<SESSION3>
CSS= 02 IID= 0D DEVICE= 0562 GROUP= "CONSOLE_003"
CONSOLE_TYPE= 2    RESPONSE= ON    READ_TIMEOUT= 60
</SESSION3>

<SESSION4>
CSS= 00 IID= 0B DEVICE= 0a61 GROUP= "CONSOLE_004"
CONSOLE_TYPE= 1    RESPONSE= OFF    READ_TIMEOUT= 30
</SESSION4>

<SESSION5>
CSS= 02 IID= 01 DEVICE= 0a62 GROUP= "CONSOLE_005"
CONSOLE_TYPE= 3    RESPONSE= ON    READ_TIMEOUT= 30
</SESSION5>

<SESSION6>
CSS= 02 IID= 08 DEVICE= 0a63 GROUP= "CONSOLE_006"
CONSOLE_TYPE= 1    RESPONSE= ON    READ_TIMEOUT= 30
</SESSION6>

<SESSION7>
CSS= 02 IID= 08 DEVICE= 0a64 GROUP= "CONSOLE_006"
CONSOLE_TYPE= 1    RESPONSE= ON    READ_TIMEOUT= 30
</SESSION7>

<SESSION8>
CSS= 02 IID= 08 DEVICE= 0a65 GROUP= "CONSOLE_006"
CONSOLE_TYPE= 1    RESPONSE= ON    READ_TIMEOUT= 30
</SESSION8>

<SESSION9>
CSS= 02 IID= 08 DEVICE= 0a66
CONSOLE_TYPE= 1    RESPONSE= ON    READ_TIMEOUT= 30
</SESSION9>

<SESSION10>
CSS= 02 IID= 08 DEVICE= 0a67 GROUP= "CONSOLE_007"
CONSOLE_TYPE= 2    RESPONSE= ON    READ_TIMEOUT= 30
DEFER_HOST_DISCONNECT= 46400
</SESSION10>

</CONFIG_SESSION>
```

**Example of a configuration file with an error**

The following is another example of a configuration file. The configuration file also includes a sample error message that you would see after validating a file and receiving a error.

```
// @@@ Error 1010: Sessions 2 and 1 are defining same device;
// i.e. same css/mifid/device
// This file has been generated from the binary file /console/data/iqzc0148.hut
// by the SE ICC Java Code on 2016.02.26-19:09:05
// Java Code Level= 605 OSA Code Version= 0
// Certificate Activate Time 2016.02.26-19:09:03
// Certificate Create Time (only full if this chpid created Certs) N/A
// Certificate Files Date created on SE2016.02.19-13:03:52

<OSC_SERVER>
<OSC_PHYSICAL_PORT0>
  HOST_IP= 10.55.1.190
  SUBNET_MASK= 255.255.255.0
  PORT= 3270
  SECURE_PORT= 3271
  HOST_LL_ADDRESS/PREFIX=  fe80::9abe:94ff:fe79:14dc/64
  ADDR_TYPE= LINK_LOCAL
  HOST_IPV6_ADDRESS/PREFIX=  fe80::9abe:94ff:fe79:14dc/64
  IPV6_PORT= 6270
  IPV6_SECURE_PORT= 6271
  ETHERNET_FRAME= DIX
  MTU= 1492
  NAME= 17C_0
</OSC_PHYSICAL_PORT0>

<OSC_PHYSICAL_PORT1>
  HOST_IP= 10.55.2.190
  SUBNET_MASK= 255.255.255.0
  PORT= 3272
  SECURE_PORT= 3273
  HOST_LL_ADDRESS/PREFIX=  fe80::9abe:94ff:fe79:14dd/64
ADDR_TYPE= LINK_LOCAL
  HOST_IPV6_ADDRESS/PREFIX=  fe80::9abe:94ff:fe79:14dd/64
  IPV6_PORT= 6272
  IPV6_SECURE_PORT= 6273
  ETHERNET_FRAME= DIX
  MTU= 1492
  NAME= 17C_1
</OSC_PHYSICAL_PORT1>
  TLS_VERSION= 1.0
  DEFAULT_GATEWAY= 10.55.1.1
  IPV6_DEFAULT_GATEWAY=  2::1
</OSC_SERVER>

<CONFIG_SESSION>
<SESSION1>
CSS= 00 IID= 01 DEVICE= 0a61 GROUP= "CONSOLE_001"
CONSOLE_TYPE= 2    RESPONSE= OFF    READ_TIMEOUT= 90
</SESSION1>

<SESSION2>
CSS= 00 IID= 01 DEVICE= 0a62 GROUP= "CONSOLE_002"
CONSOLE_TYPE= 1    RESPONSE= ON    READ_TIMEOUT= 90
DEFER_HOST_DISCONNECT= 86400
</SESSION2>
```

## 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. There can be no space between the tag and the ‘=’ sign.
3. There must be a space immediately after the ‘=’ sign.
4. Tags can be placed in any order given that they are within the bounds of their delimiters.

5. Server tags must be within the server delimiters.
6. 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 identifier descriptions**

**//**
This indicates that any text until 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.

**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, 10.21.1.228). This address is assigned to the OSA-ICC server, and this is the address that TN3270E clients will be connecting to. The following is an example of using this tag: HOST_IP= 10.21.1.228. This tag is required for configuration and there is no default value.

**PORT=**
The server's port. The port number on which the OSA3270 server will be listening (accepting) non-secure clients. For example, PORT= 3270. It is acceptable to use any valid port number the integer range 1 to 65535. This is a required tag for server configuration. Setting this value to 0 will block non-secure connections to this OSA-ICC physical port.

**HOST_LL_ADDRESS/PREFIX**
An auto-generated Link Local address and prefix.

**ADDR_TYPE=**
The Address Type string can have two vaues: STATIC or LINK_LOCAL.

**HOST_IPV6_ADDRESS/PREFIX=**
User-configured IPv6 address and prefix that can be a Link local or static IPv6 address.

**IPV6_PORT, IPV6_SECURE_PORT=**
Port numbers to be used for opening IPv6 Non-SSL and SSL listen servers.

**SUBNET_MASK=**
Subnet mask of the network to which the OSA ICC server is connected.

**ETHERNET_FRAME=**
Specifies the Ethernet standard SNAP versus DIX.

**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 576.

**NAME=**
The name can be up to 15 characters and is not case sensitive. Acceptable input characters include ASCII values in the range 0x21 through 0x7E. See Appendix A, “ASCII table,” on page 103 for more information. This tag is required for configuration and there is no default value. It is displayed in the 3 line logo. See “Logo Controls” on page 54.

**TLS_VERSION**
Indicates the minimum TLS protocol version supported by the PCHID. It is configurable via the config source file by giving protocol version 1.0, 1.1, and 1.2. There is only one per adapter.

**DEFAULT_GATEWAY**
Only one per adapter.

**IPV6_DEFAULT_GATEWAY**
IPv6 default gateway to be configured.

**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.

**</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.

**CSS=**
The channel subsystem number. The valid range is 0-5. 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 Appendix A, “ASCII table,” on page 103. This tag is required for configuration and there is no default value.

**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, 10.21.1.252. Specifying a CLIENT_IP is optional. However, omitting this tag r will allow any client to connect to a specific session.

**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 no timeout for deferment will be enforced. 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.

**Note:** Each z/OS Master Console input/output console session, with the DHD option enabled: Must have a unique LU name to ensure session auto-reconnection and MSC console recovery occurs correctly. See “LU Name” in “Display client connections” on page 22.

**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.

**Note:** It is highly recommended to set Response Mode on, RESPONSE= 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 5-300 seconds. This tag is optional in file configuration.

**Note:**

1. 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.
2. For secure sessions, the recommended value for this parameter is 90. For non-secure sessions, the recommended value for this parameter is 60.

**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.

**Important Note**: If you try to activate a configuration that has validation errors in it, the configuration file will be returned to the last good configuration. Validation Warnings are allowed (return code < 1000 are considered warnings). Configurations with warnings can be successfully activated.

## Validating a manual configuration file

1. From the ***OSC manual configuration*** window 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 an error” on page 42. For a list of errors that you might receive, see Chapter 11, “Error and warning messages,” on page 91. Here is the window you will see if your source file has errors:

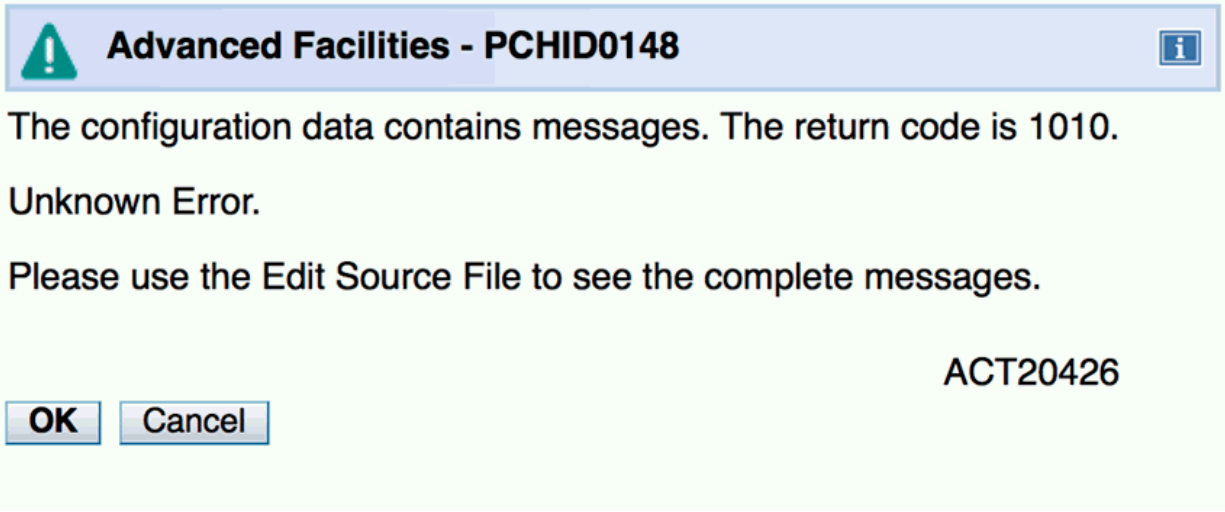



*Figure 29. OSC validate source file window*

You must fix all errors (return code 1000 or greater) 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.

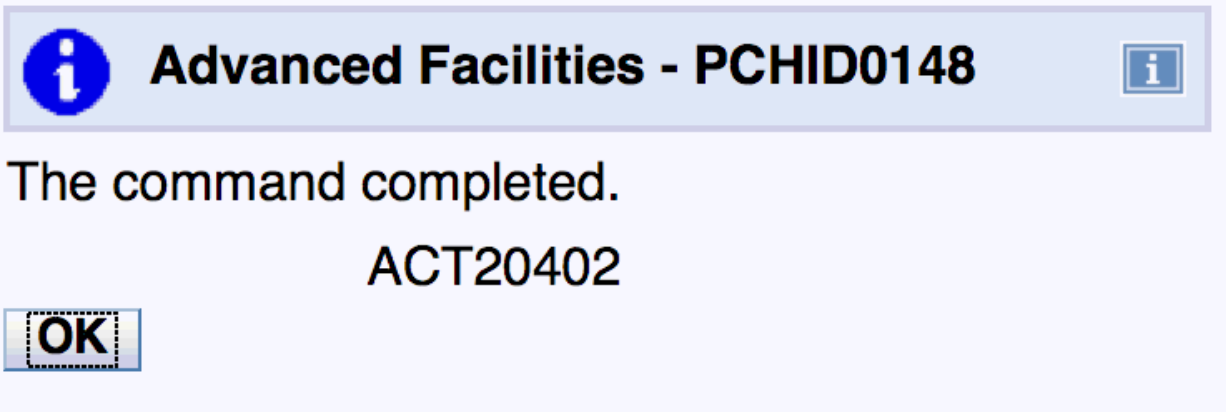



*Figure 30. Successful validate source file*

## Activate configuration

The ***Activate configuration*** window is used to activate a valid session configuration file. If you choose to activate a configuration file, connected sessions that have pending configuration changes will disconnect and then reconnect with the new configuration options in effect if the emulator's auto reconnect feature is enabled.

**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.

**Important Note**: If you try to activate a configuration that has validation errors in it, the configuration file will be returned to the last good configuration. Validation Warnings are allowed (return code < 1000 are considered warnings). Configurations with warnings can be successfully activated.

**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.

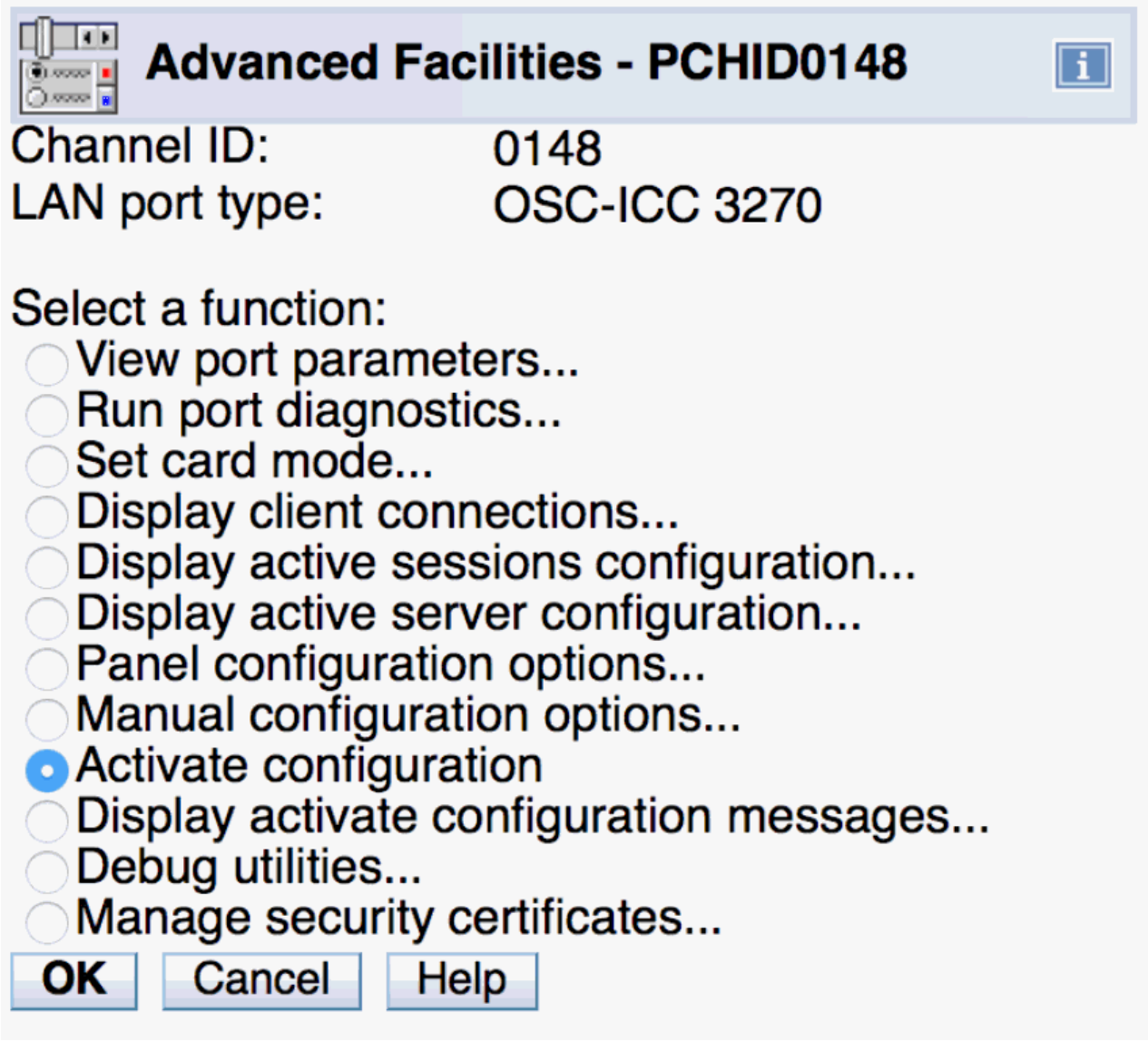



*Figure 31. Activate configuration window*

## Display activate configuration errors

The ***Display activate configuration errors*** window 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.

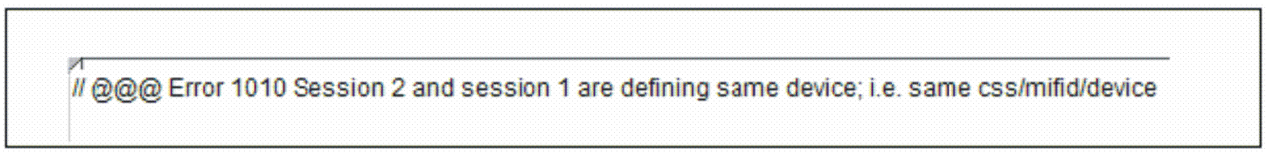



*Figure 32. Display activate configuration errors window*

For a list of possible errors and warnings, see Chapter 11, “Error and warning messages,” on page 91.

# Chapter 7. Debug utilities

The ***Debug utilities*** window is the high level selection window 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.

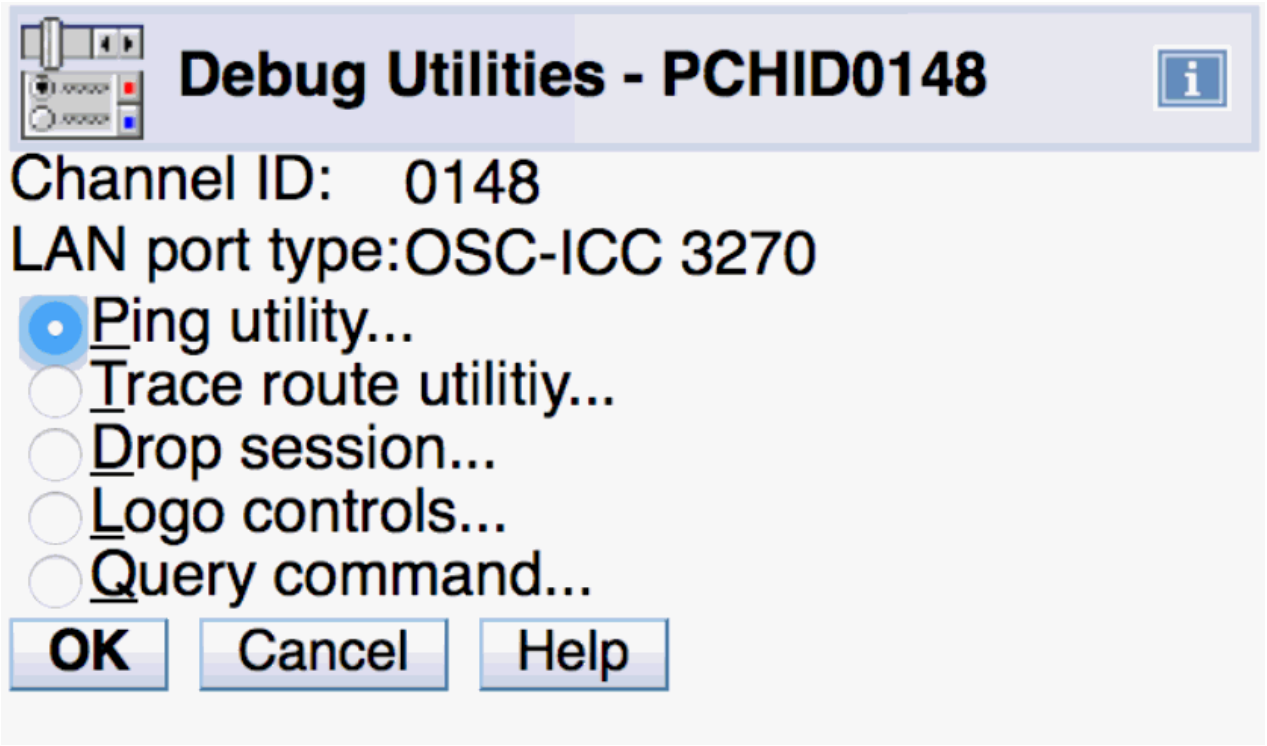



*Figure 33. Debug utilities window*

## Ping Utility

The ***Ping Utility*** window 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.

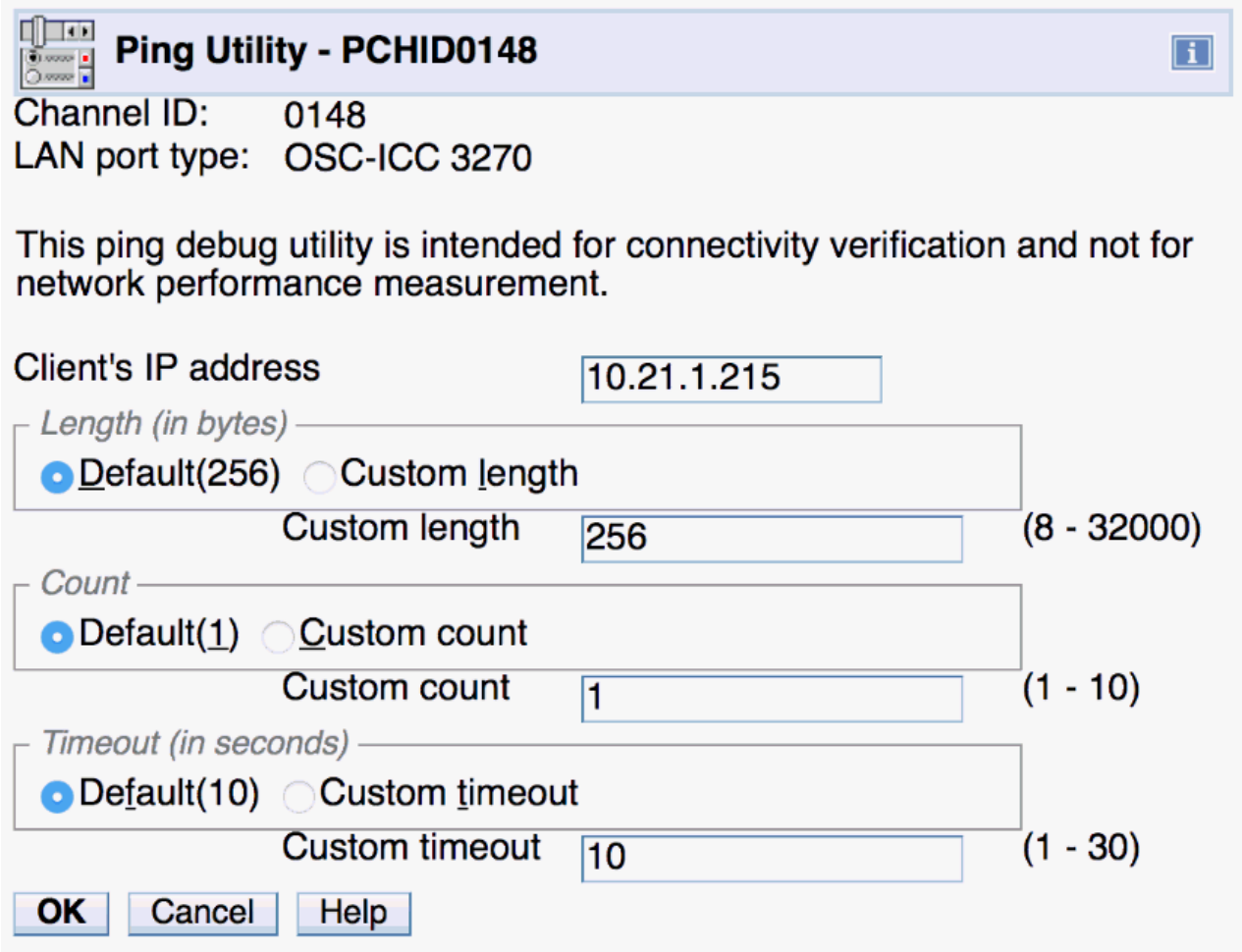



*Figure 34. Ping Utility*

The Ping utility requires the following input:

- Client's IP address (IPv4 or IPv6): 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.

The Ping utility issues the following response:

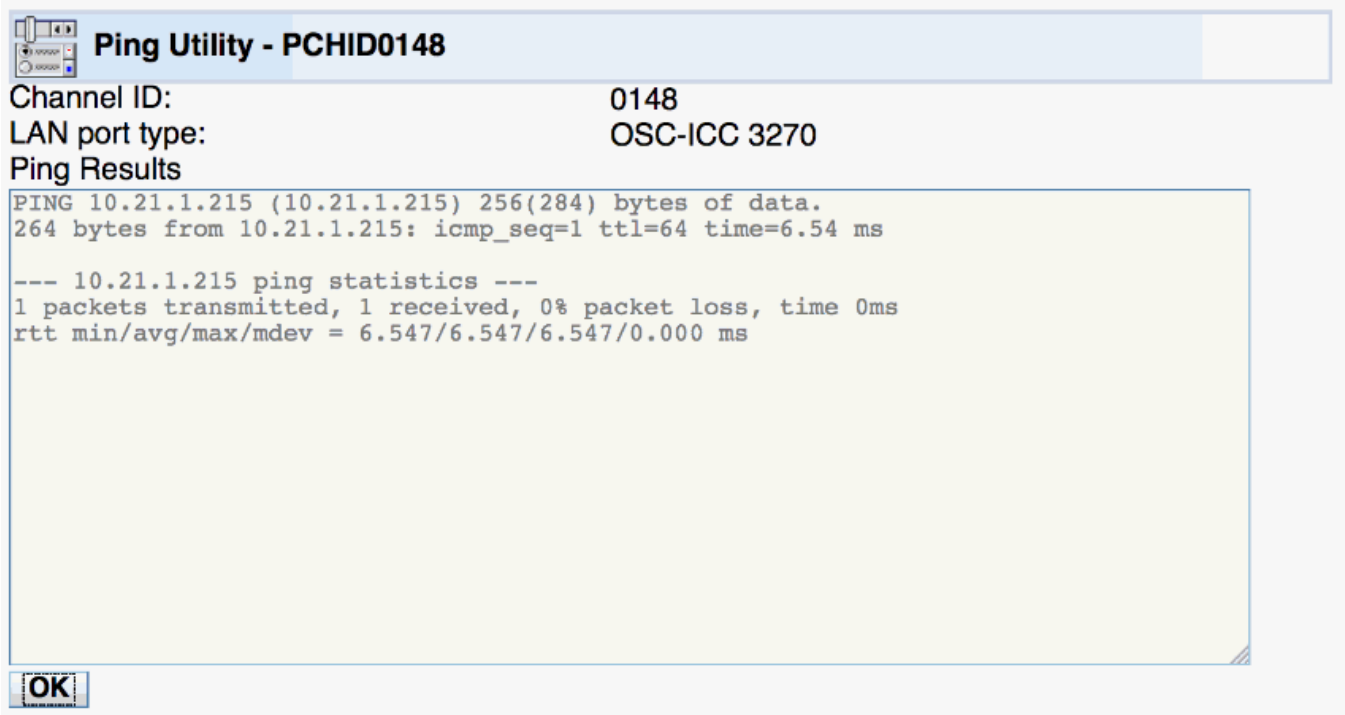



*Figure 35. Ping Utility response*

## Trace route utility

The ***Trace route utility*** window 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.

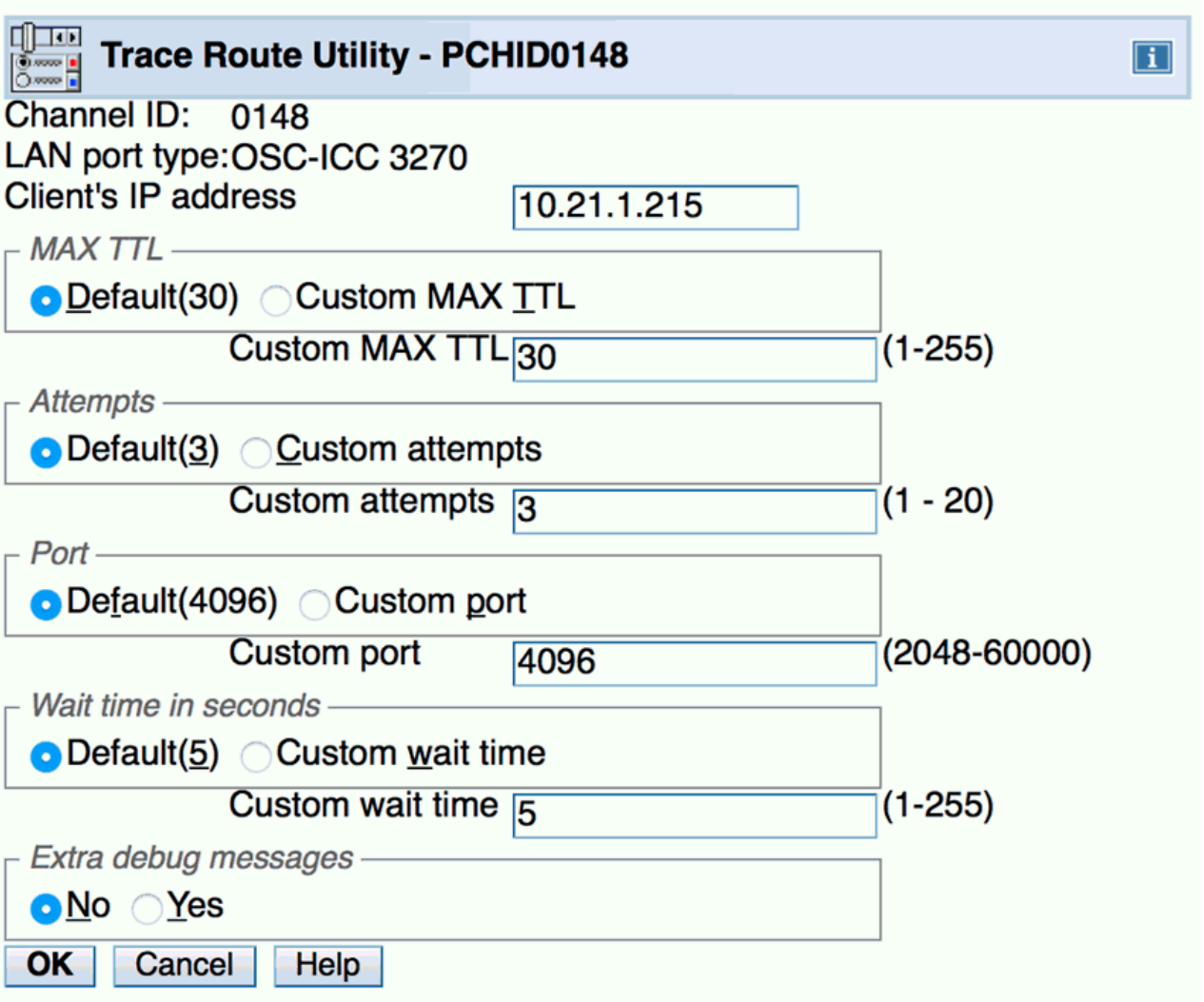



*Figure 36. Trace route utility*

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.

The trace route utility issues the following output:

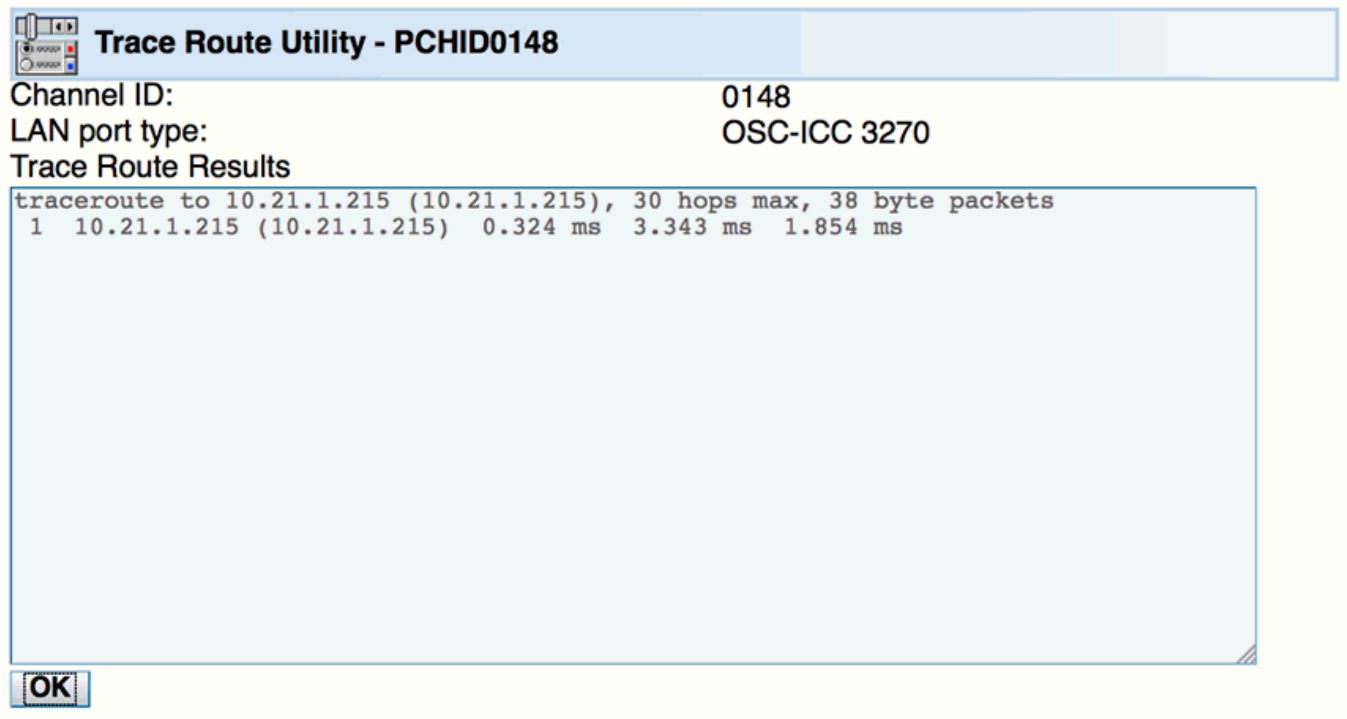



*Figure 37. Trace route utility output*

## Drop session

The ***Drop session*** window is used to drop a session from an OSA-ICC. You can use this window if you need to drop a session because you can't get to a client 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.

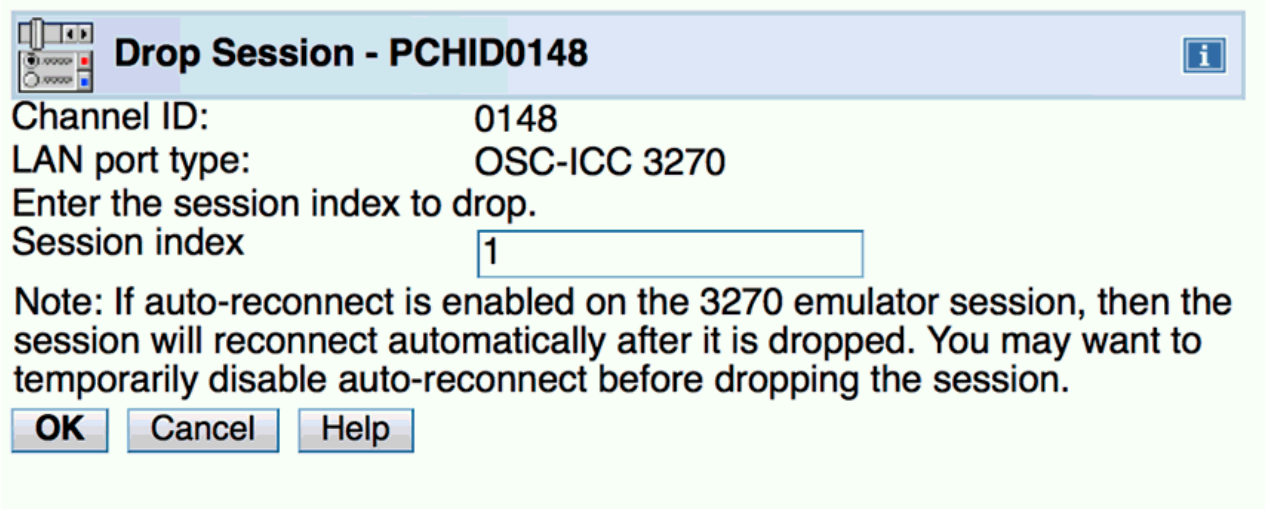



*Figure 38. Drop session utility*

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

The drop session window requires the following input:

- Session index: specifies the session number. This is always the LT Index + 1.

## Logo Controls

The ***Logo Controls*** window is used to enable or disable the 3 line logo sent to the client on initial telnet negotiation success – Please refer to Figure 59 on page 80.

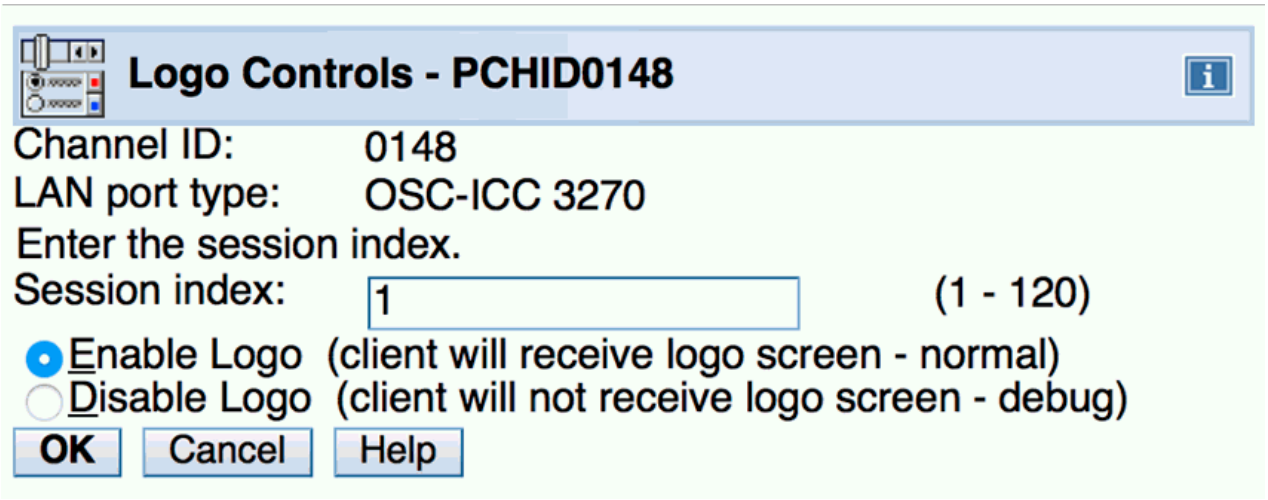



*Figure 39. Logo Controls*

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

Depending on the version of ICC Firmware you might have the following set of available commands.

- help – get the list of supported commands
- arp – display osa arp table
- route – display osa network route table
- osass – display socket list – z13 GA2
- osaps – display osa process list – z13 GA2
- osals – display files
- osaps – display active processes
- ip6nebr – display IPv6 neighbors mac address – z14 GA2
- route6 – display IPv6 route table – z14 GA2

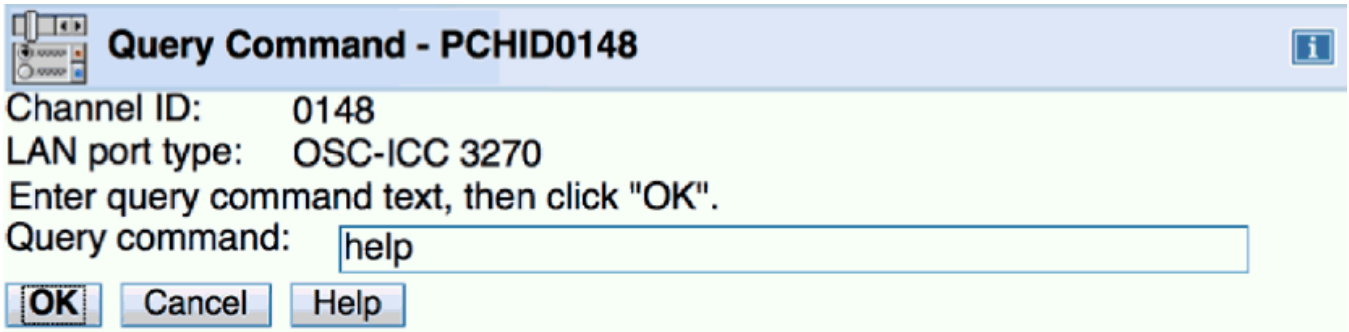



*Figure 40. Query command*

The query command utility requires an input command. Some commands may require additional input parameters. For a list of supported commands type `help`. A supported command is further explained by entering `help` then the command name.

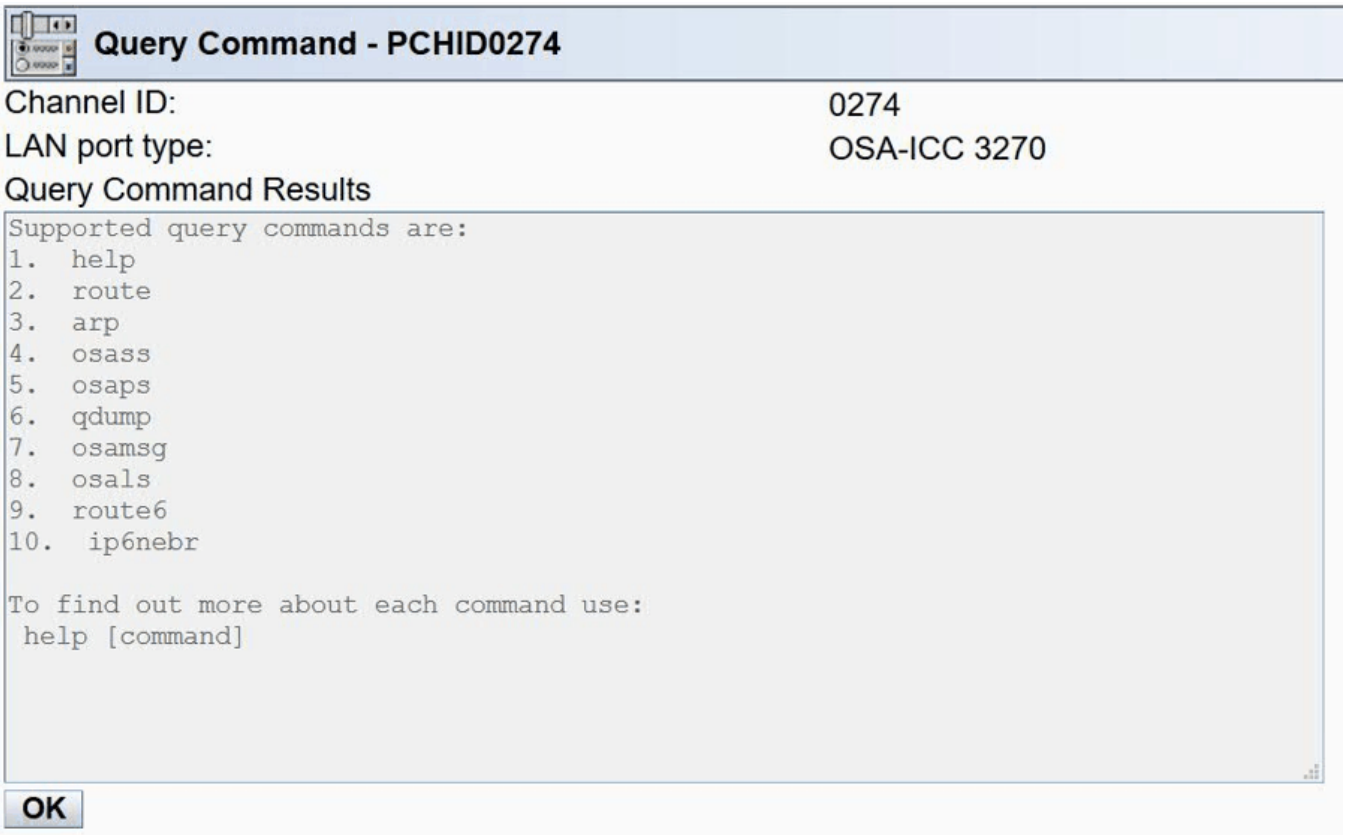



*Figure 41. Query command help information*

The query command window requires the following input:

- Name of command
- Command parameters

The results of a query command are displayed on a window after successful execution of that command.

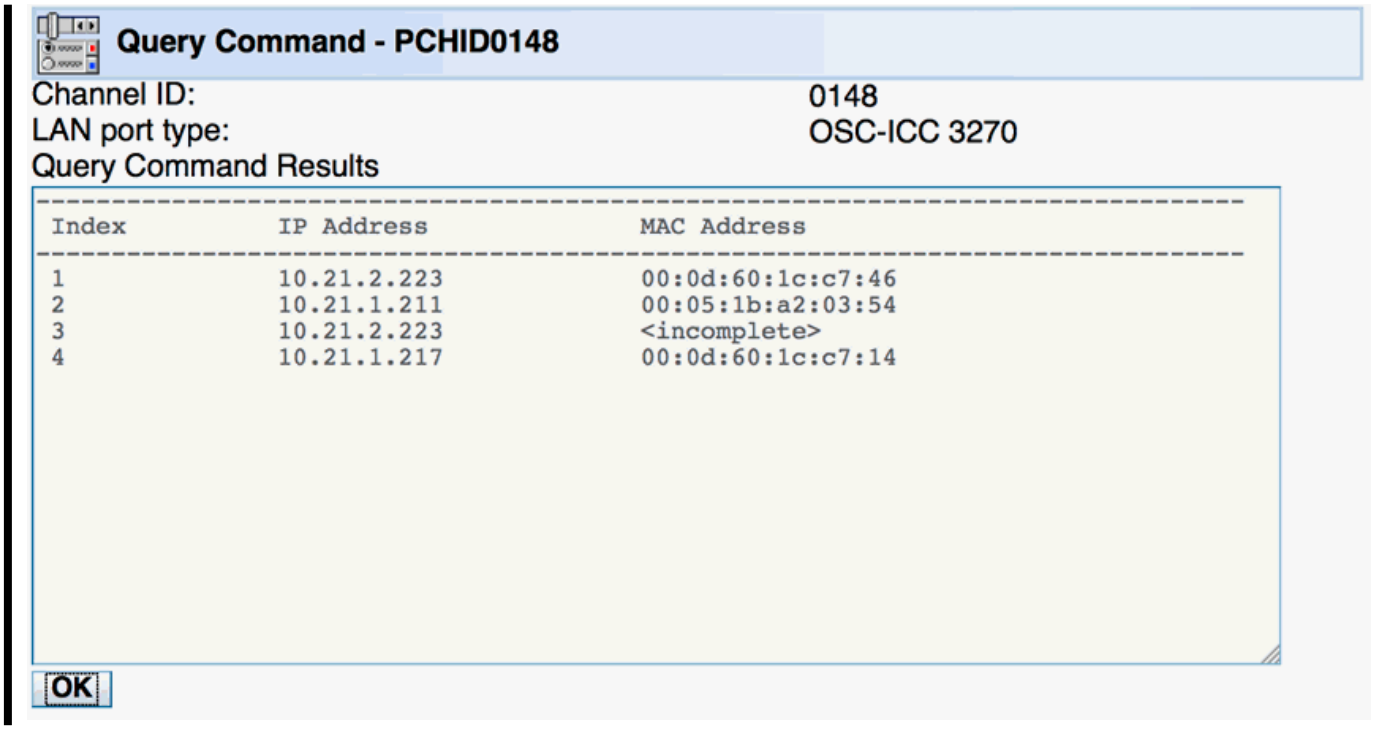



*Figure 42. Query arp command output*

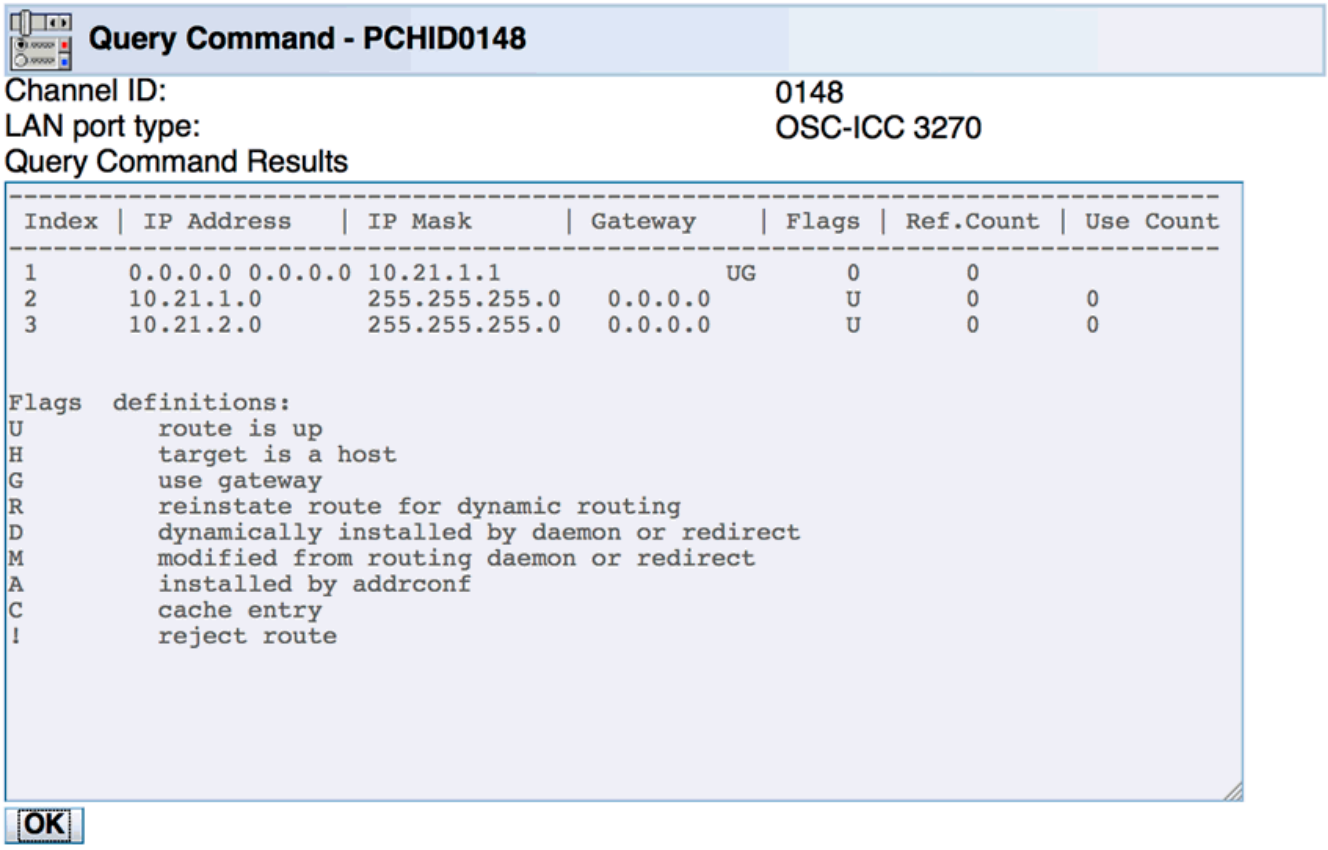



*Figure 43. Query command output for route*

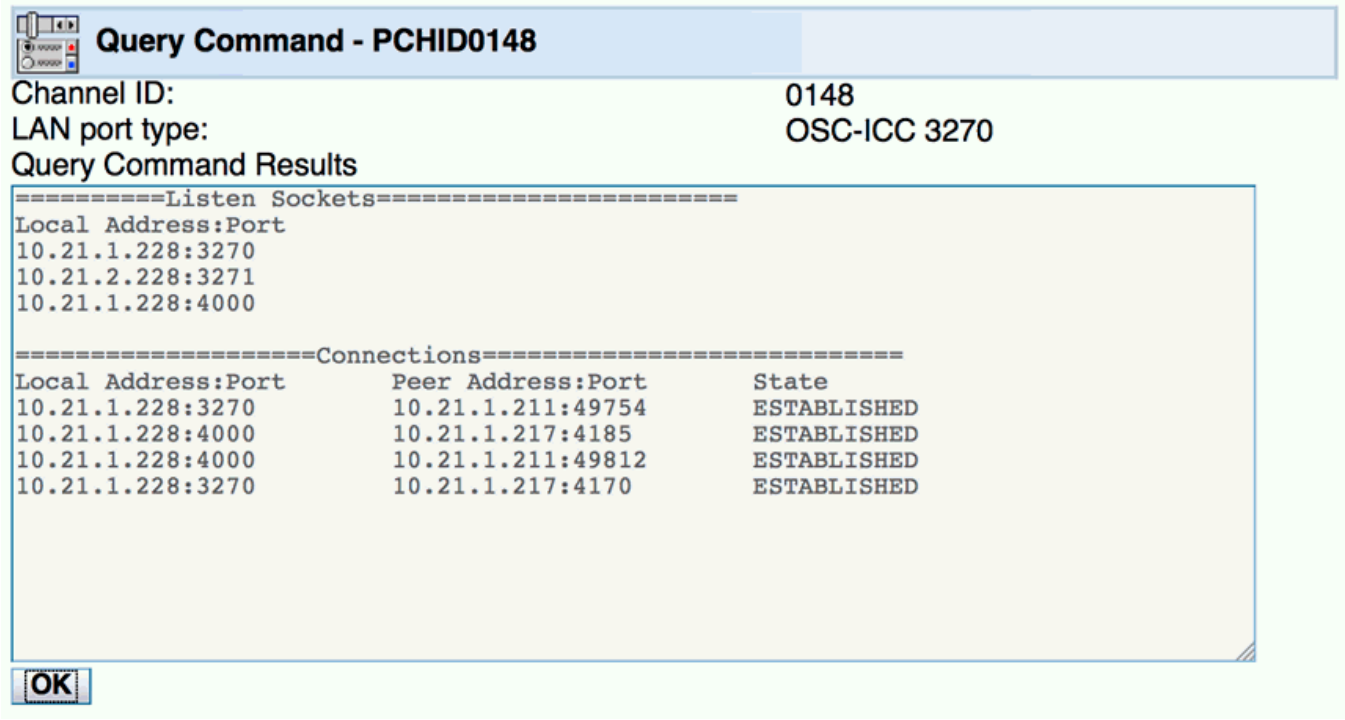



*Figure 44. Query command output for osass*

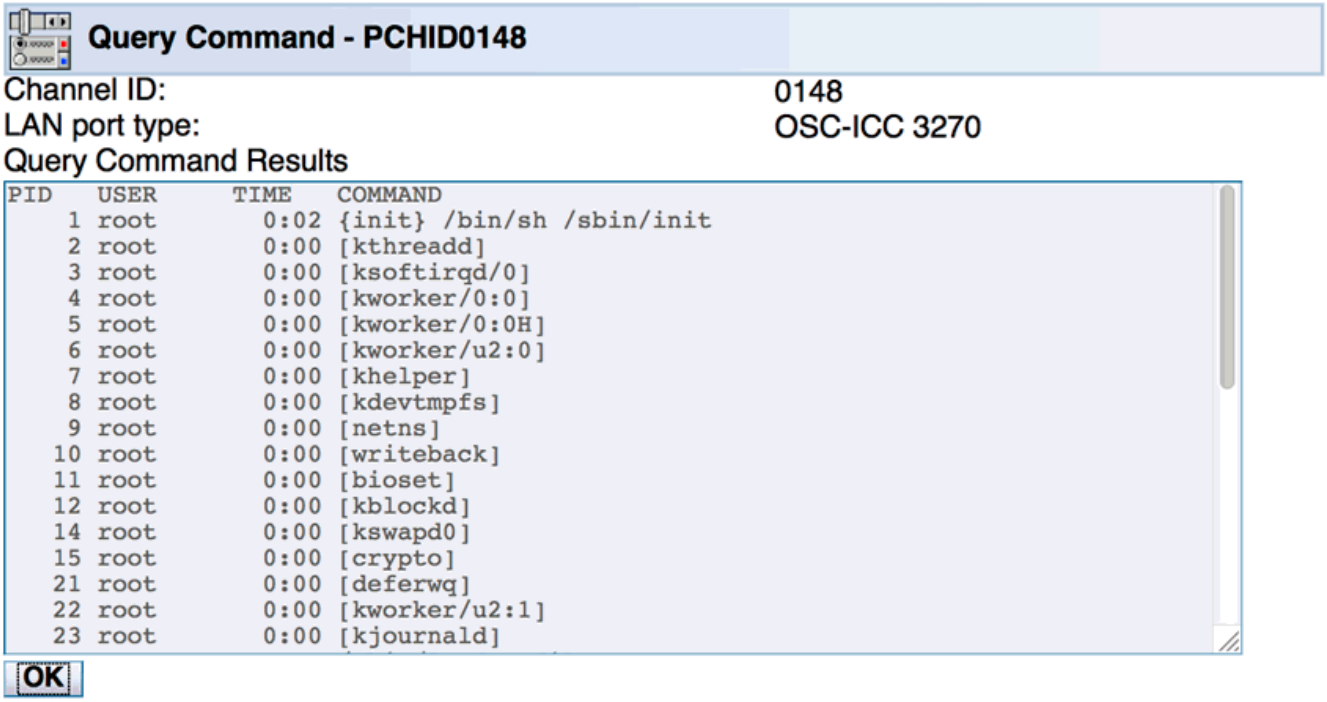



*Figure 45. Query command output for osaps*

# Chapter 8. OSA-ICC TLS Encrypted Session Support

Beginning with z13 GA2, OSA -ICC provides Transport Layer Security (TLS) encrypted session support to the OSA-ICC adapter. TLS is a widely used protocol which provides privacy between two communicating applications (generally a client and a server). With the TLS support in OSA-ICC, clients are authenticated through X.509 public key certificates. TLS requires an underlying transport protocol (usually TCP/IP) for data transmission and reception. The TLS protocol can be used to negotiate an encryption algorithm and session key before a client application transmits or receives data. Once the session key is negotiated, data is exchanged encrypted.

Key management (RSA) takes place during the TLS session "handshake". For RSA, a pre-master secret is encrypted using the server's public-key and sent by the client to the server. The pre-master secret is decrypted by the server using the server's private-key, so that client and server then share the pre-master secret. The pre-master secret is used to generate the symmetric key used for data transmission over the TLS session.

OSA-ICC provides:

- Encryption of data for privacy and integrity
- Tunneling of other TCP/IP-based sessions (such as TN3270e) over encrypted channels.

**Note:** OSA-ICC supports certificates of up to 16 KB.

## x.509 Certificate Management

Limited OSA-ICC TLS key management is provided. A single key, self-signed X.509 certificate, and certificate request is stored on the password protected SE and in the configuration information stored on the OSA adapter. The customer is expected to manage and secure additional certificates if required.

The certificate and key are protected by checksum and date on the closed SE system. The checksum and date are verified every time the key/certificate is loaded by the OSA-ICC adapter.

OSA-ICC Encryption Assumptions (subject to change as enhanced protocols and encryption methods become available):

- Support both per PCHID certificate and per Z system certificate
- Support will be provided for Transport Layer Security - TLS1.0, TLS1.1, and TLS 1.2
- 256 (Secure Hash Algorithm) SHA-2 with 2048 bit RSA key to be used for the handshake/certificate validation
- Advanced Encryption Standard (AES) AES-128 is the only cipher supported for the session key versus support is provided for certificates signed by a trusted CA or self-signed
- CA-signed certificate formats supported are .pem and .p7b
- Only one self-signed certificate will be generated per system (not per OSC CHPID or card) – stored in .pem format
- Enablement of secure ports will be done at the SE/HMC, and will only be allowed if the CPACF facility is enabled
- Self-signed certificates [Per chpid and Renewed system wide certificate] have 10-year expiration
- Only server side authentication is supported (no client authentication)
- If TLS-encrypted sessions are supported by the OSA-ICC , the Manage Security Certificates panel are available.

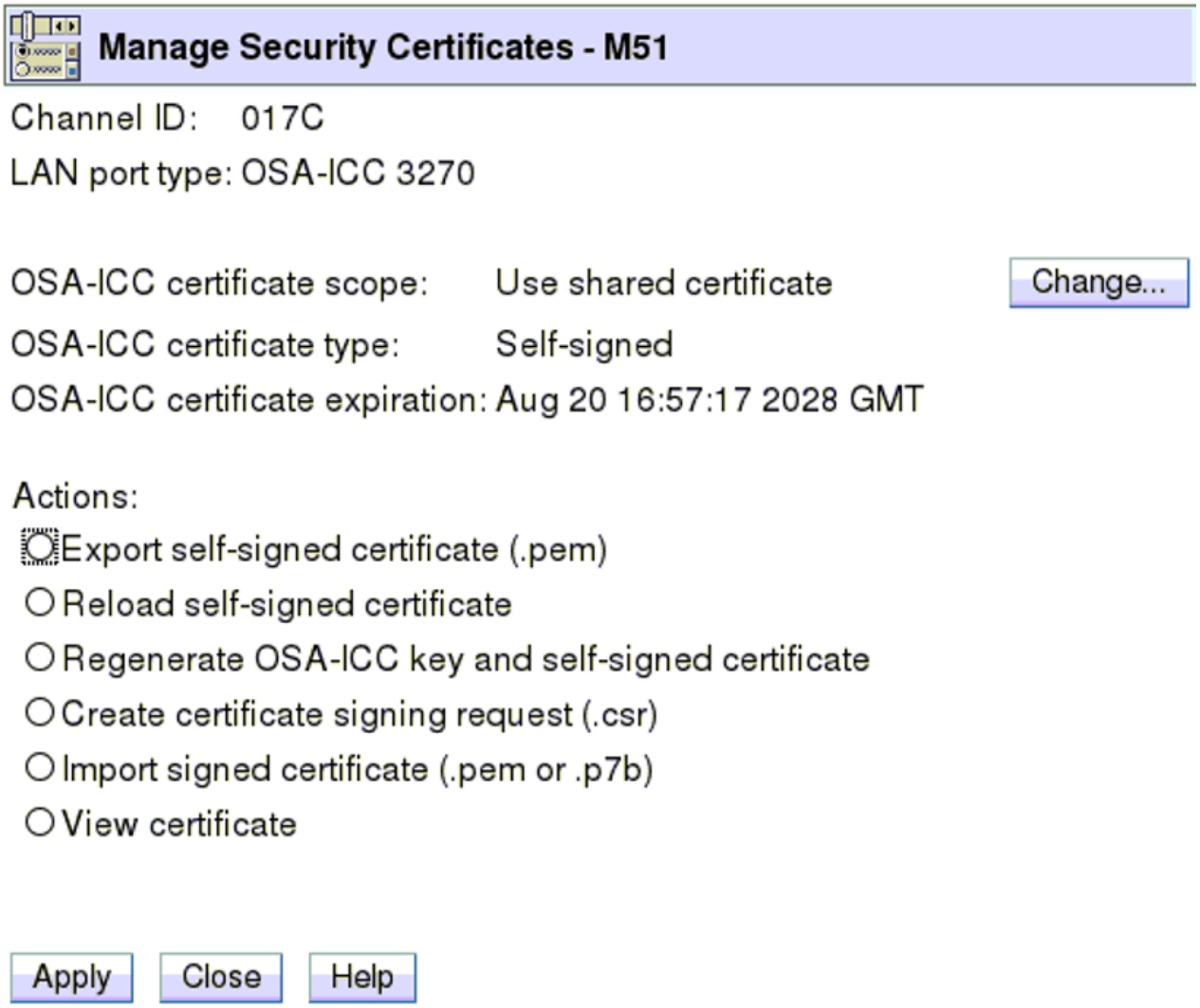



*Figure 46. Manage Security Certificates window*

The new functions will be used to verify that all PCs connecting to the Secure TCP port have the appropriate keys to manage the data flow between the connections.

The following functions are supported:

**OSA-ICC Certificate Scope**
The scope of the currently Installed certificate on the PCHID. And It will have either of the two values from Self-signed or Certificate Authority (CA)-signed.

**OSA-ICC Certificate Type**
The type of the currently Installed certificate on the PCHID. And It will have either of the two values from self signed or CA signed values.

**OSA-ICC Certificate Expiration**
The expiration date of the currently installed certificate on the PCHID.

**Export Self Signed Certificate**
On first Initialization, the OSA SE microcode generates a self Signed Certificate and stores it in the configuration file and on the SE disk. When you click this button, the SE copies the file off of the SE disk and places it on a USB device or ready for ftp/sftp to an external server. By default, this certificate is loaded onto the OSA-ICC when a secure port is defined in the server configuration window.

**Reload Self-Signed Certificate**
Using this option, you can reload the self-signed certificate. That is, if the current scope is Individual, then per CHPID self-signed certificate is reloaded; likewise, if it shares certificate scope, then shared self-signed certificate will be reloaded.

**Create Certificate Signing Request**
On first Initialization, the OSA SE microcode generates a Certificate Signing Request and stores it in the configuration file and on the SE disk. When you click this button, the SE copies the file off the SE disk and places it on a USB device or ready for ftp/sftp to an external server. This file could then be sent to an external CA to create a certificate or used to generate a local certificate by an in-house certificate generation program. The resulting certificate is imported to the OSA via the "Import Certificate" function.

**Import Signed Certificate**
Using this option, you can import the CA signed certificate on to PCHID. Supported formats are only .pem or .p7b.

**View Certificate**
Using this option, you can view the currently installed active certificate contents.

If the certificate changes or expires, all connections established are terminated.

To enable this function you must configure a Secure Port in the Server Configuration window, and then apply the appropriate certificate to your client. For a client using the OSA generated self-signed certificate you must export the self signed certificate to your client, import that certificate into your workstations certificate management software, and point your client to the secure socket number. See Chapter 10, "eNetwork Personal Communications (PCOMM) configuration," on page 77 for an example of how to set this up for Pcomm.

## Cancel command

The ***Cancel Command utility*** window allows you to cancel an I/O command that is executing on an OSC.

## Manage Security Certificates panel with edit certificate feature

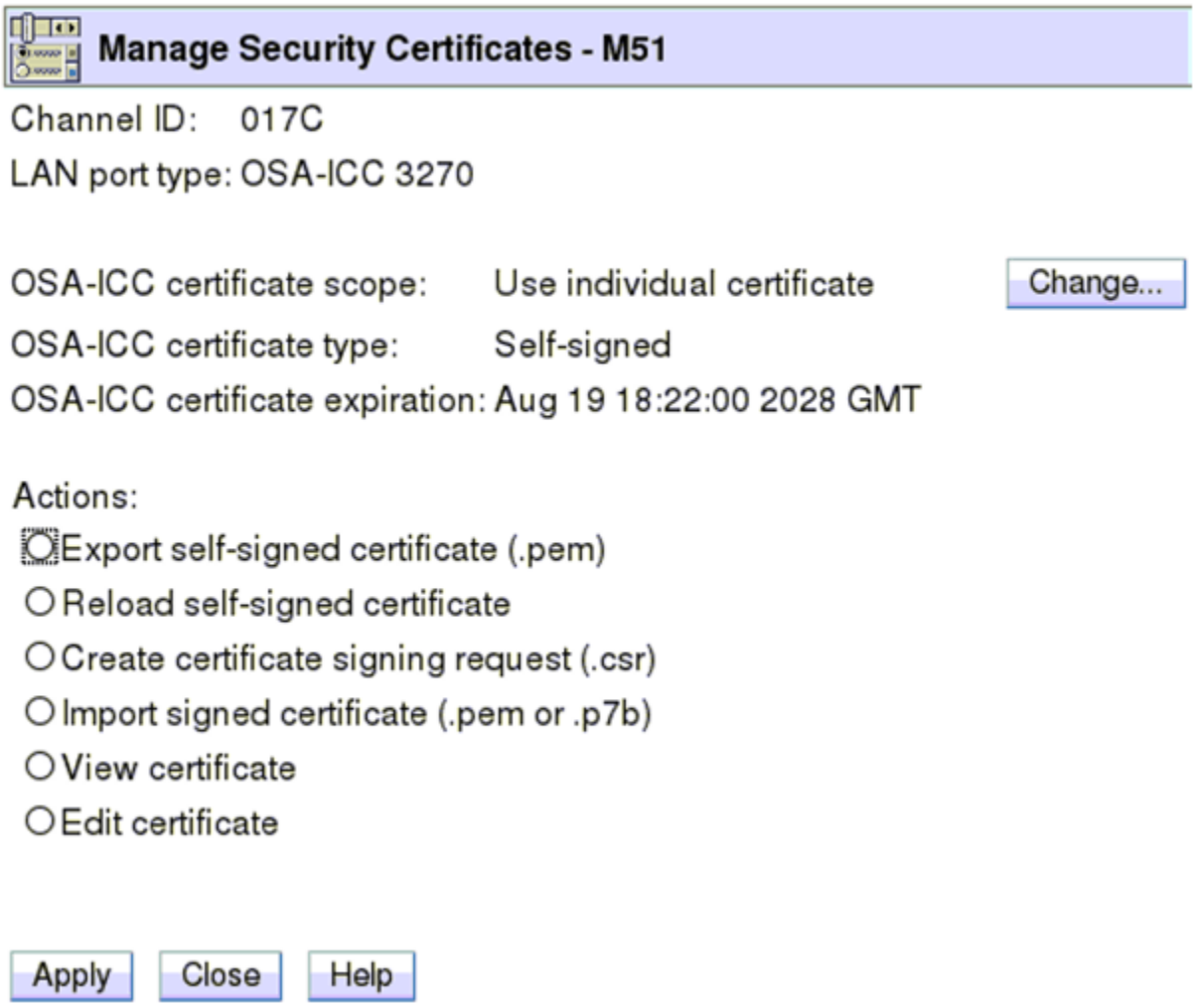



*Figure 47. Manage Security Certificates window*

**Edit Certificate**

This option is available whenever the active certificate installed on the PCHID is with Individual scope. Using this option, you can edit the given certificate with the respective organization specific requirements. Edit certificate feature is supported for the Individual Certificate scope with self signed or CA signed certificate type values. Modifying and saving the certificate attributes terminates all of the existing console connections.

If the certificate changes or expires, all connections established are terminated.

## Using a shared self-signed certificate

To configure TLS on OSA-ICC with a self-signed certificate:

1. Enter a non 0 value into the Secure Port Number for one or both of the OSA-ICC physical ports.
   a. You can do this via the Window or Manual Configuration Options
2. Validate the Configuration
3. Activate the Configuration
4. Enter the Manage Security Certificate Window
5. Select Export Self-Signed Certificate –
   a. Export via USB or FTP

**Note:** Be sure to specify a filetype of .pem.

6. Copy Self-Signed Certificate to Workstation being configured for TLS encryption
7. On Client Workstation - Import Self-Signed Certificate into Certificate Management Software provided on the Workstation (program will be unique to OS or emulator used. See Certificate management on your Workstation's Operating System or Application Software for more details)
8. Setup Workstation TN3270e emulator parameters
    a. Configure OSA-ICC IP
    b. Secure Port Number
    c. Lu Name (Group Name)
    d. Select TLS version and FIPS mode (if applicable)
9. Connect TN3270e Client

## Using an externally signed certificate with a shared certificate scope

To configure TLS on OSA-ICC with an externally signed certificate:

1. Enter a non 0 value into the Secure Port Number for one or both of the OSA-ICC physical ports.
    a. You can do this via the Window or Manual Configuration Options
2. Validate the Configuration
3. Activate the Configuration
4. Enter the Manage Security Certificate Window
5. Select Export Certificate Signing Request
    a. Export via USB or FTP
6. Copy Certificate Request to Workstation or USB media to provide to external CA or to generate your own certificate by running through a local Certificate generator. Certificate Signing request fields cannot be modified.
7. Obtain CA or locally signed certificate in .pem or .p7b format
    a. Place on media or workstation to import into OSA-ICC and Client Workstation
8. On OSA-ICC - Select Import certificate
    a. Import via USB or FTP
9. On Client Workstation - Import CA or locally signed Certificate into Certificate Management Software provided on the Workstation (program will be unique to OS or emulator used. See Certificate management on your Workstation's Operating System or Application Software for more details)
10. Setup Workstation TN3270e emulator parameters
    a. Configure OSA-ICC IP
    b. Secure Port Number
    c. Lu Name (Group Name)
    d. Select TLS version and FIPS mode (if applicable)
11. Connect TN3270e Client

## Switching from an external certificate to a shared self-signed certificate

To return to a self-signed certificate:

1. Enter the Manage Security Certificate window
2. Select Reload Self-Signed Certificate

3. Select Export Self-Signed Certificate
   a. Export via USB or FTP
4. Copy Self-Signed Certificate to Workstation being configured for TLS encryption
5. On Client Workstation - Import Self-Signed Certificate into Certificate Management Software provided on the Workstation (program will be unique to OS or emulator used. See Certificate management on your Workstation's Operating System or Application Software for more details)
6. Setup Workstation TN3270e emulator parameters
   a. Configure OSA-ICC IP
   b. Secure Port Number
   c. Lu Name (Group Name)
   d. Select TLS version and FIPS mode (if applicable)
7. Connect TN3270e Client

## Using an individual self-signed certificate

To configure TLS on OSA-ICC with a self-signed certificate:

1. Consider Non zero secure port is defined on the PCHID and shared self signed certificate is active
2. On the Manage Security Certificates window, change the scope from the shared certificate to individual certificate scope.

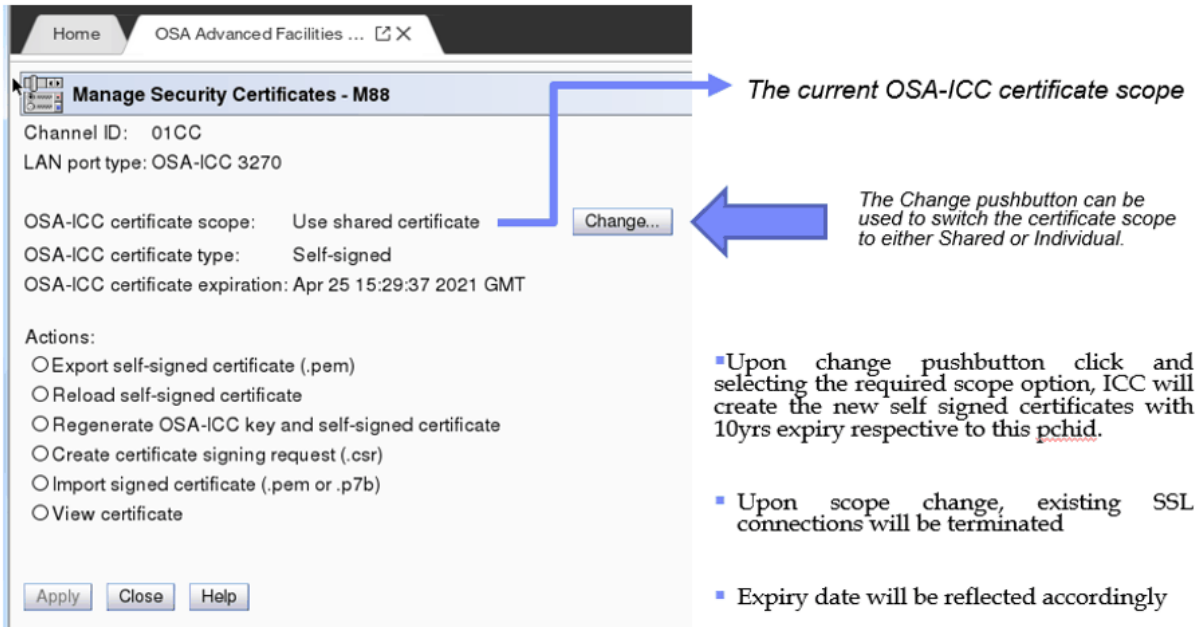



*Figure 48. Manage Security Certificates window*

3. Change OSA ICC Certificate scope

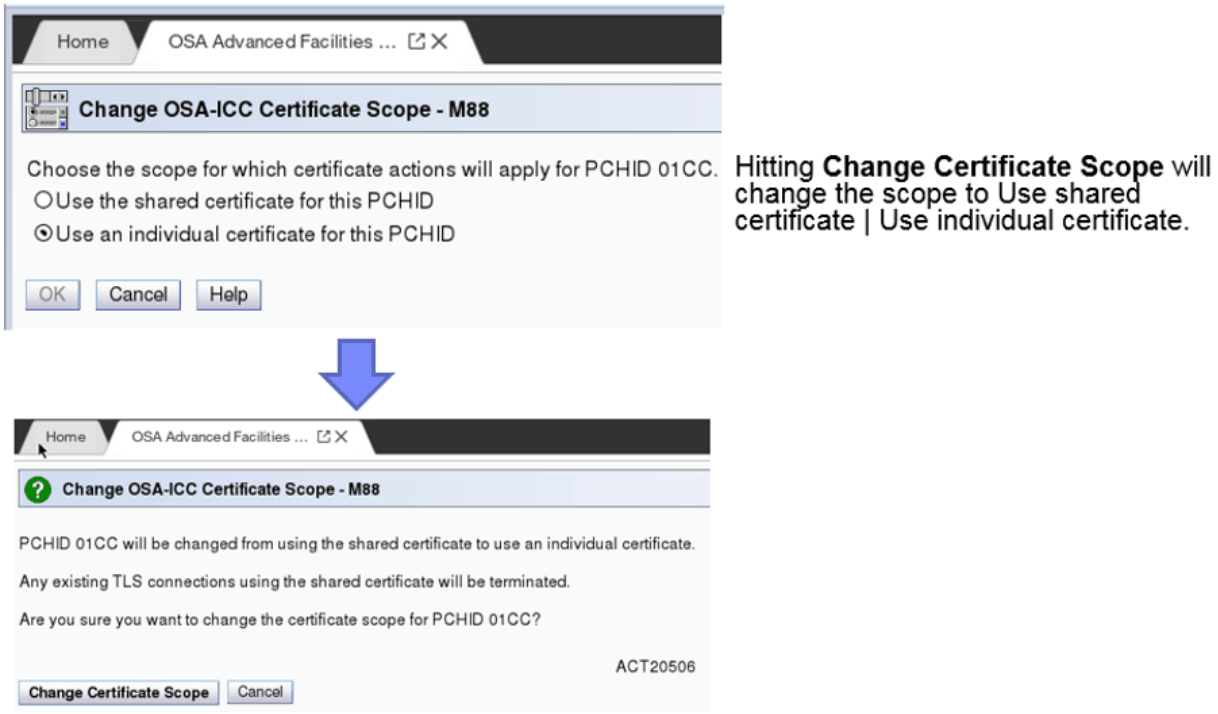



*Figure 49. Change OSA-ICC Certificate Scope*

4. Select Export Self-Signed Certificate –
   a. Export via USB or FTP

      **Note:** Be sure to specify a filetype of .pem.
5. Copy Self-Signed Certificate to Workstation being configured for TLS encryption
6. On Client Workstation - Import Self-Signed Certificate into Certificate Management Software provided on the Workstation (program will be unique to OS or emulator used. See Certificate management on your Workstation's Operating System or Application Software for more details).
7. Set up Workstation TN3270e emulator parameters
   a. Configure OSA-ICC IP
   b. Secure Port Number
   c. Lu Name (Group Name)
   d. Select TLS version and FIPS mode (if applicable)
8. Connect TN3270e Client

## Using an individual self-signed certificate with modifying attributes

To configure TLS on OSA-ICC with a self-signed certificate:

1. Consider the PCHID is using default individual self-signed certificate i.e perform the steps given in "Using an individual self-signed certificate"

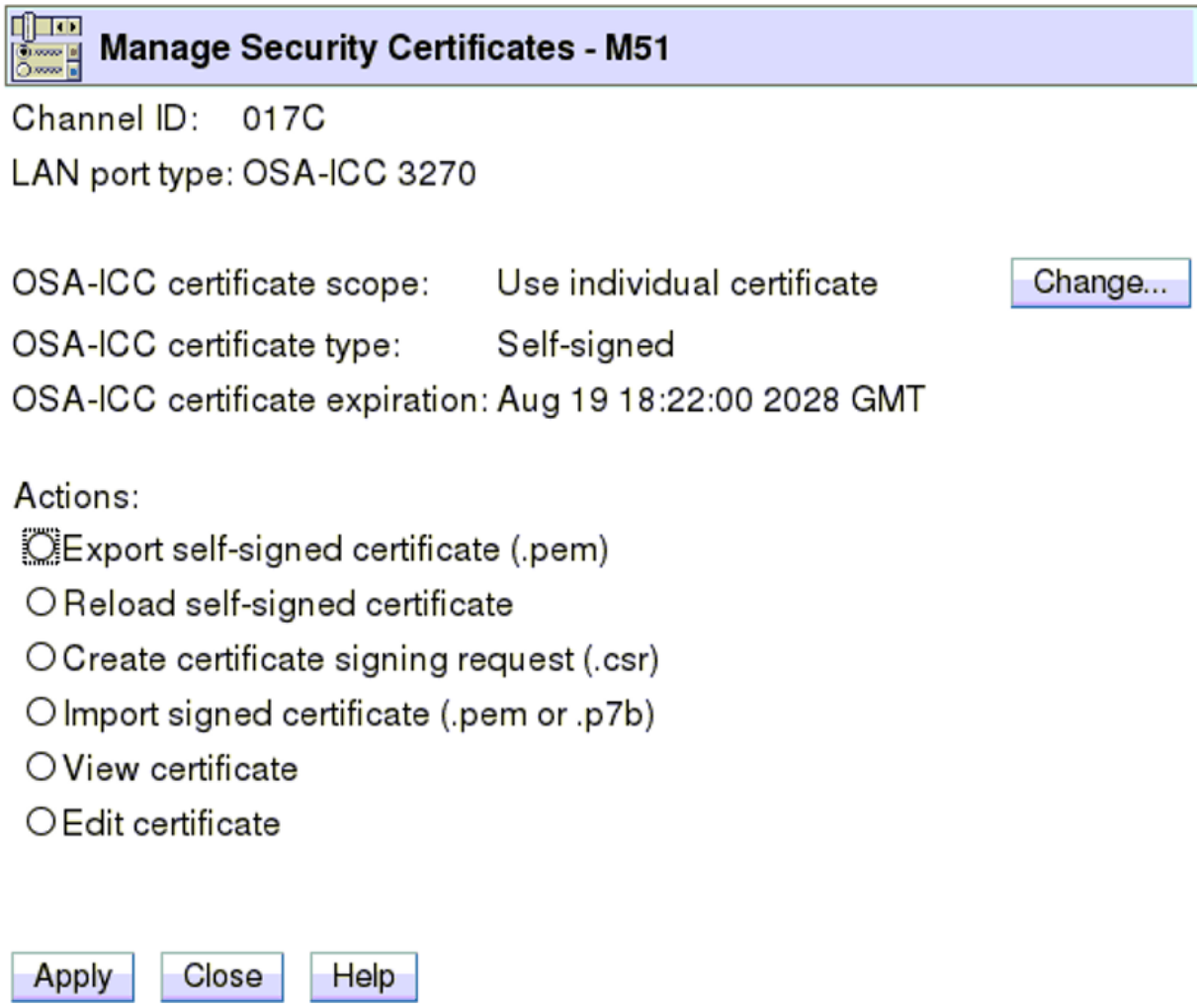



*Figure 50. Manage Security Certificates window*

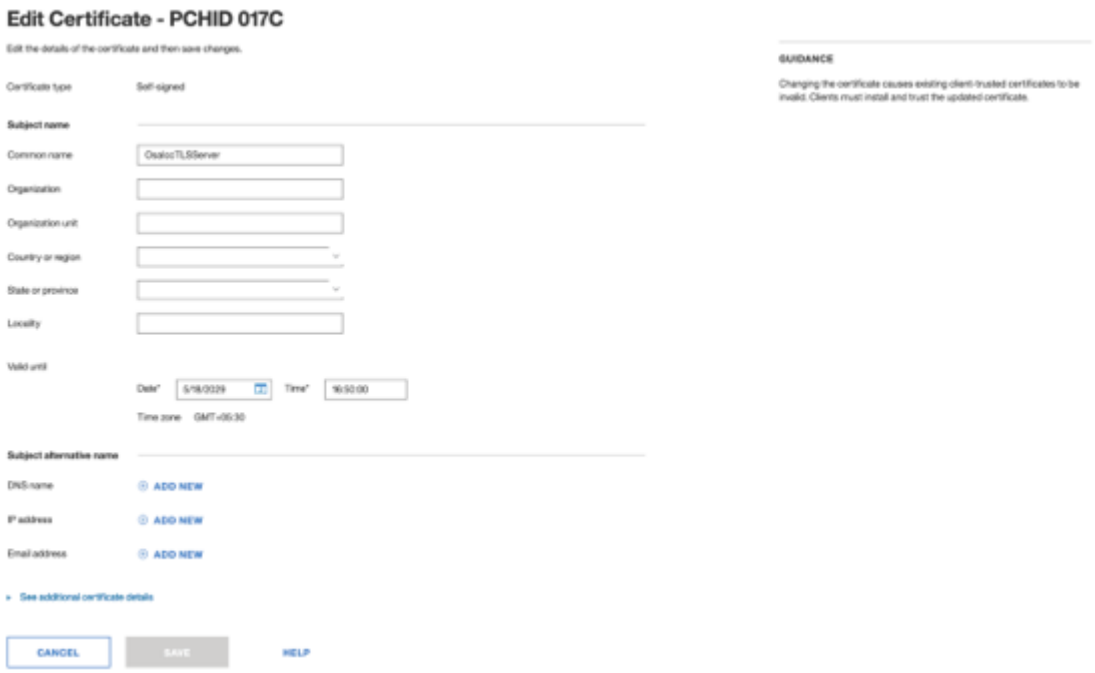



*Figure 51. Edit Certificate window*

2. Enter Manage security certificates panel.
3. Select the Edit Certification option and it will allow the user to enter all the below certificate signing request attributes
   a. Common name,
   b. Organization,
   c. Organization unit,
   d. Country or region,
   e. State or province, Locality
   f. And Subject Alternative Names like IP address, DNS name and Email address
4. After editing the attributes, click Save.


*Figure 52. Save certificates changes confirmation*

5. Click continue, the certificate update progress appears, follows by the save successful Informational message.

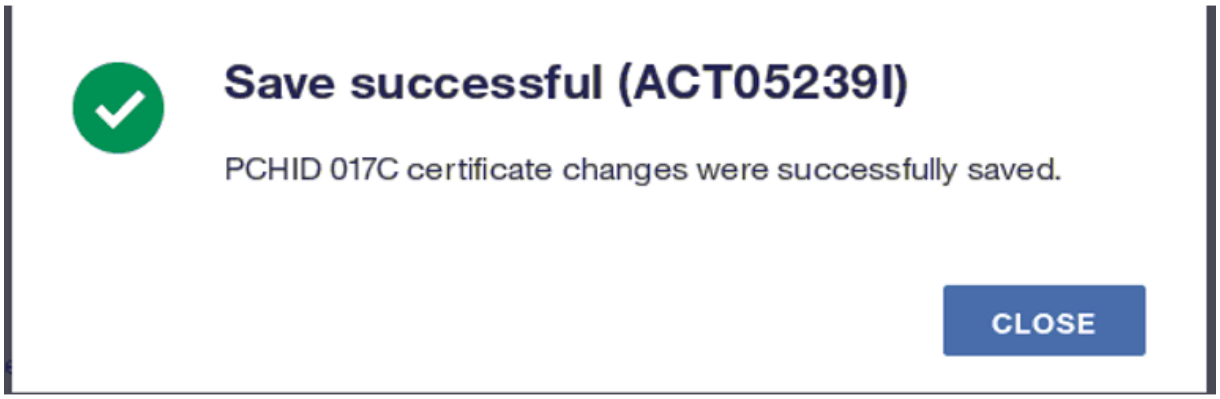



*Figure 53. Save successful message*

6. Click CLOSE to return to the Manage Security Certificates window.
7. Select View Certificate and confirm that the certificate got updated with the Step 3 changes.
8. Select Export Self-Signed Certificate –
   a. Export via USB or FTP

   **Note:** Be sure to specify a filetype of .pem.
9. Copy Self-Signed Certificate to Workstation being configured for TLS encryption
10. On Client Workstation - Import Self-Signed Certificate into Certificate Management Software provided on the Workstation (program will be unique to OS or emulator used. See Certificate management on your Workstation's Operating System or Application Software for more details).
11. Set up Workstation TN3270e emulator parameters
    a. Configure OSA-ICC IP
    b. Secure Port Number
    c. Lu Name (Group Name)
    d. Select TLS version and FIPS mode (if applicable)
12. Connect TN3270e Client

## Using an externally signed certificate with an individual certificate scope

This scenario is applicable to both individual certificate with modified attributes or default individual self-signed attributes:

1. Consider the PCHID is defined and is active with either external CA signed or individual self signed certificate
2. Select Export Certificate Signing Request
   a. Export via USB or FTP
3. Copy Certificate Request to Workstation or USB media to provide to external CA or to generate your own certificate by running through a local Certificate generator.
4. Obtain CA or locally signed certificate in .pem or .p7b format.
   a. Place on media or workstation to import into OSA-ICC and Client Workstation
5. On OSA-ICC - Select Import certificate
   a. Export via USB or FTP
6. On Client Workstation - Import CA or locally signed Certificate into Certificate Management Software provided on the Workstation (program will be unique to OS or emulator used. See Certificate management on your Workstation's Operating System or Application Software for more details)
7. Setup Workstation TN3270e emulator parameters

a. Configure OSA-ICC IP
b. Secure Port Number
c. Lu Name (Group Name)
d. Select TLS version and FIPS mode (if applicable)

8. Connect TN3270e Client

## Using an externally signed certificate with modifying attributes

To use an externally signed certificate with modifying attributes:

1. Consider the PCHID is using default individual self-signed certificate i.e perform the steps given in "Using an individual self-signed certificate"
2. Enter Manage security certificates panel.


*Figure 54. Manage Security Certificates window*

3. Select the Edit Certification option and it will allow the user to enter all the below certificate signing request attributes
   a. Common name,
   b. Organization,
   c. Organization unit,
   d. Country or region,
   e. State or province, Locality
   f. Subject Alternative Names like IP address, DNS name and Email address
4. Modify the required attributes for the externally signed certificate and click Next button
5. Next export certificate signing request panel pops up so either choose FTP or USB media to get the modified certificate signing request.

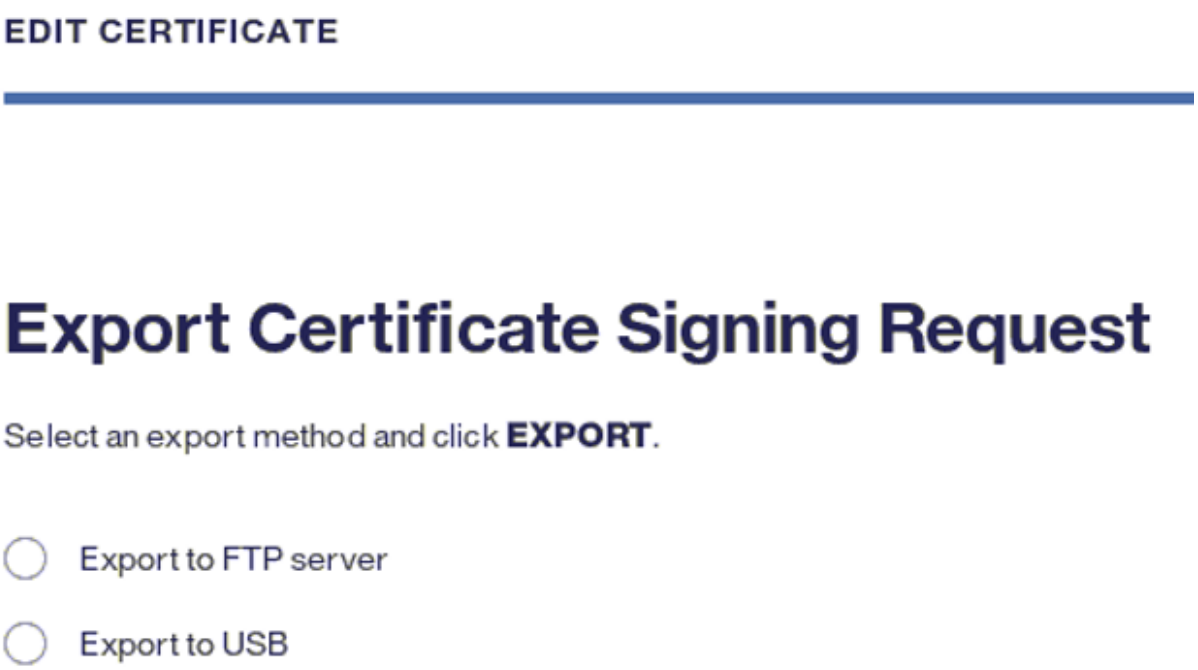



*Figure 55. Export Certificate Signing Request*

6. Copy this modified Certificate Signing Request to Workstation or USB media to provide to external CA or to generate your own certificate by running through a local Certificate generator
7. With the above steps, the existing console sessions will not be disconnected.
8. Obtain CA or locally signed certificate in .pem or .p7b format
    a. Place on media or workstation to import into OSA-ICC and Client Workstation
9. On OSA-ICC - Select Import certificate
    a. Import via USB or FTP
10. On Client Workstation - Import CA or locally signed Certificate into Certificate Management Software provided on the Workstation (program will be unique to OS or emulator used. See Certificate management on your Workstation's Operating System or Application Software for more details).
11. Set up Workstation TN3270e emulator parameters
    a. Configure OSA-ICC IP
    b. Secure Port Number
    c. Lu Name (Group Name)
    d. Select TLS version and FIPS mode (if applicable)
12. Connect TN3270e Client

## View self-signed certificate

This action enables you to view such currently installed certificate contents as Common name, Issuer details, Certificate validity, and encryption thumb print.

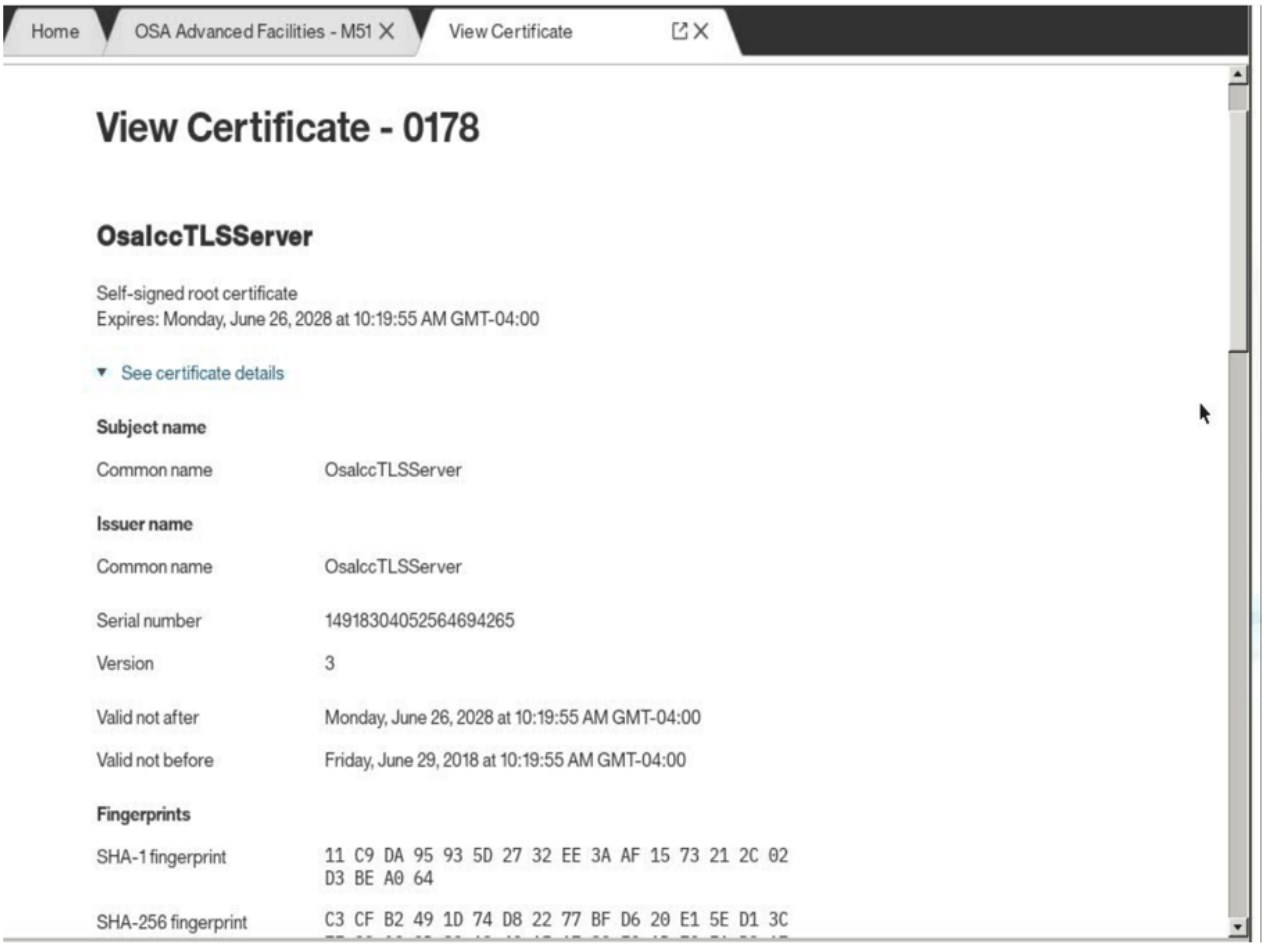



*Figure 56. Certificate view*

## Switching from an external certificate to an Individual self-signed

To return to an individual self-signed certificate:

1. Consider the PCHID is defined and is active with either external CA signed or individual self signed certificate.
2. Enter the Manage Security Certificate window.
3. Select Reload Self-Signed Certificate.
4. Select Export Self-Signed Certificate.
   a. Export via USB or FTP.
5. Copy Self-Signed Certificate to Workstation being configured for TLS encryption.
6. On Client Workstation - Import Self-Signed Certificate into Certificate Management Software provided on the Workstation (program will be unique to OS or emulator used. See Certificate management on your Workstation's Operating System or Application Software for more details.).
7. Set up Workstation TN3270e emulator parameters.
   a. Configure OSA-ICC IP
   b. Secure Port Number
   c. Lu Name (Group Name)
   d. Select TLS version and FIPS mode (if applicable).
8. Connect TN3270e Client.

## Switching from an individual self-signed to a shared self-signed (switch certificate scope)

To return to system wide shared self signed certificate:

1. Consider secured port is defined and is active with either external CA signed or individual self signed certificate.
2. Enter the Manage Security Certificate window.
3. Select Reload Self-Signed Certificate.
4. Select Export Self-Signed Certificate.
   a. Export via USB or FTP.
5. If the client work station is not installed with shared self signed certificate then follow the steps (a and b) below; otherwise, go to the next step.
   a. Copy Self-Signed Certificate to Workstation being configured for TLS encryption.
   b. On Client Workstation - Import Self-Signed Certificate into Certificate Management Software provided on the Workstation (program will be unique to OS or emulator used. See Certificate management on your Workstation's Operating System or Application Software for more details.).
6. Set up Workstation TN3270e emulator parameters.
   a. Configure OSA-ICC IP
   b. Secure Port Number
   c. Lu Name (Group Name)
   d. Select TLS version and FIPS mode (if applicable).
7. Connect TN3270e Client.

## Supported cipher suites

**TLSv1.0**

Ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A

Compressors:

NULL
Cipher preference: client

**TLSv1.1**

Ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A

Compressors:

NULL
Cipher preference: client

**TLSv1.2**

Ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) – A
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A

Compressors:

NULL
Cipher preference: client
Least strength: A
MAC address: 98:BE:94:79:14:DC (IBM)

# Chapter 9. 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.

# Chapter 10. eNetwork Personal Communications (PCOMM) configuration

For recommended PCOMM levels for OSA-ICC, see “Recommended PCOMM levels” on page 2.

The following is an example of defining a PCOMM 3270 session. The example uses PCOMM version 6.014 for Windows. If you are using a different version, your windows 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.

## Defining a PCOMM TN3270E session

**About this task**

Start from the Windows desktop - Operating System Level Dependent

**Procedure**

1. Select **Programs** --> **IBM Personal Communications** --> **Start or Configure Sessions**

   The IBM Personal Communication (PCOMM) Session Manager window is displayed.
2. Click **New Session**

   The Customized Communication window is displayed:

   - **Type of Host** zSeries
   - **Interface** LAN
   - **Attachment** Telnet3270

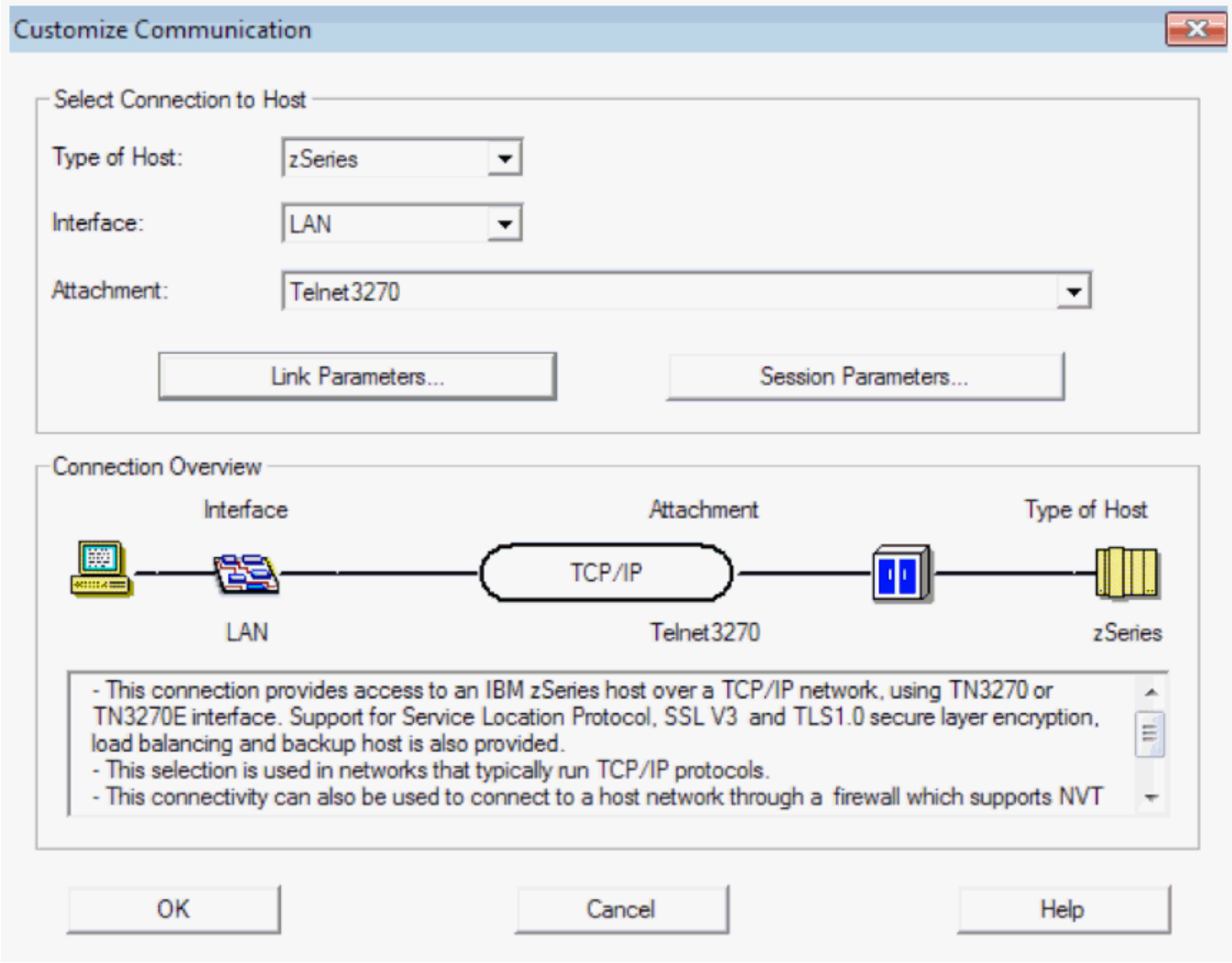



*Figure 57. Customize Communication window*

3. Click **Link Parameters**
4. Define the connection from the workstation to the OSA-ICC server.

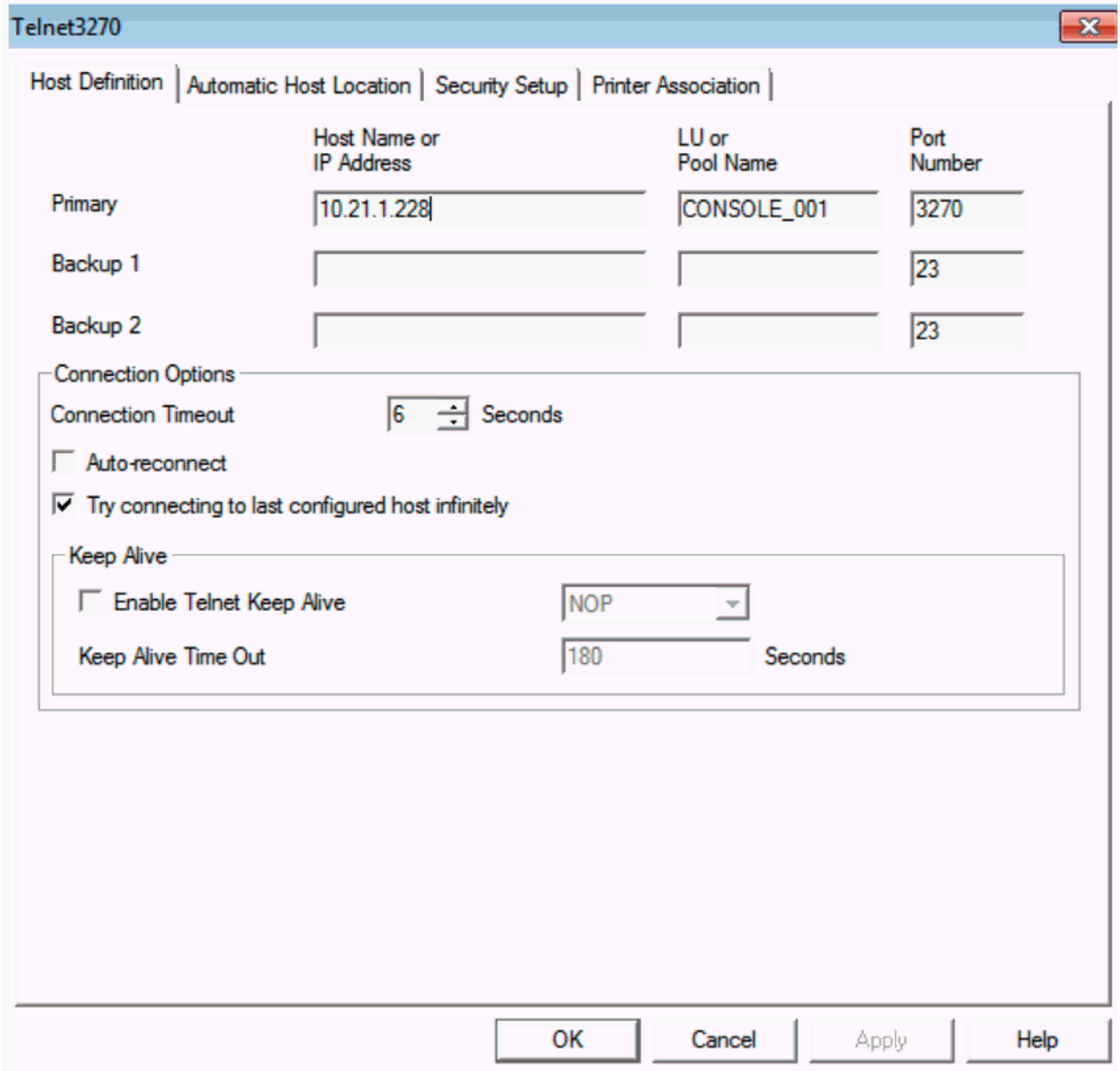



*Figure 58. Telnet3270 window*

5. 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 27.

6. Enter the Port Number.

   This must match the Port Number (either secure or non-secure) in the OSA-ICC Configuration

7. Enter the LU or Group Name.

   This must match the LU name in the OSA-ICC server configuration.

8. Click OK on the Telnet3270 window.

   **Note:**

   a. It is recommended that you select auto-reconnect. However, understand that the drop session option for configuring an OSA-ICC will not work as expected. 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 53.

b. z/OS Master Console input/output console session, with the DHD option enabled:

- Must have the auto-reconnect function enabled.
- Must have a unique LU name to ensure session auto-reconnection and MSC console recovery occurs correctly. See “LU Name” in “Display client connections” on page 22.

---

**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.

For z/OS:

- Display type 3277 model 2 has a screen size of 24 rows by 80 columns.
- Display type 3277 model 3 has a screen size of 32 rows by 80 columns.

See your VTAM definitions for z/OS and your Operating System console definitions for more details.

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

If the host session is ready for communication, the screen displayed shows your connection information for this session. For example:

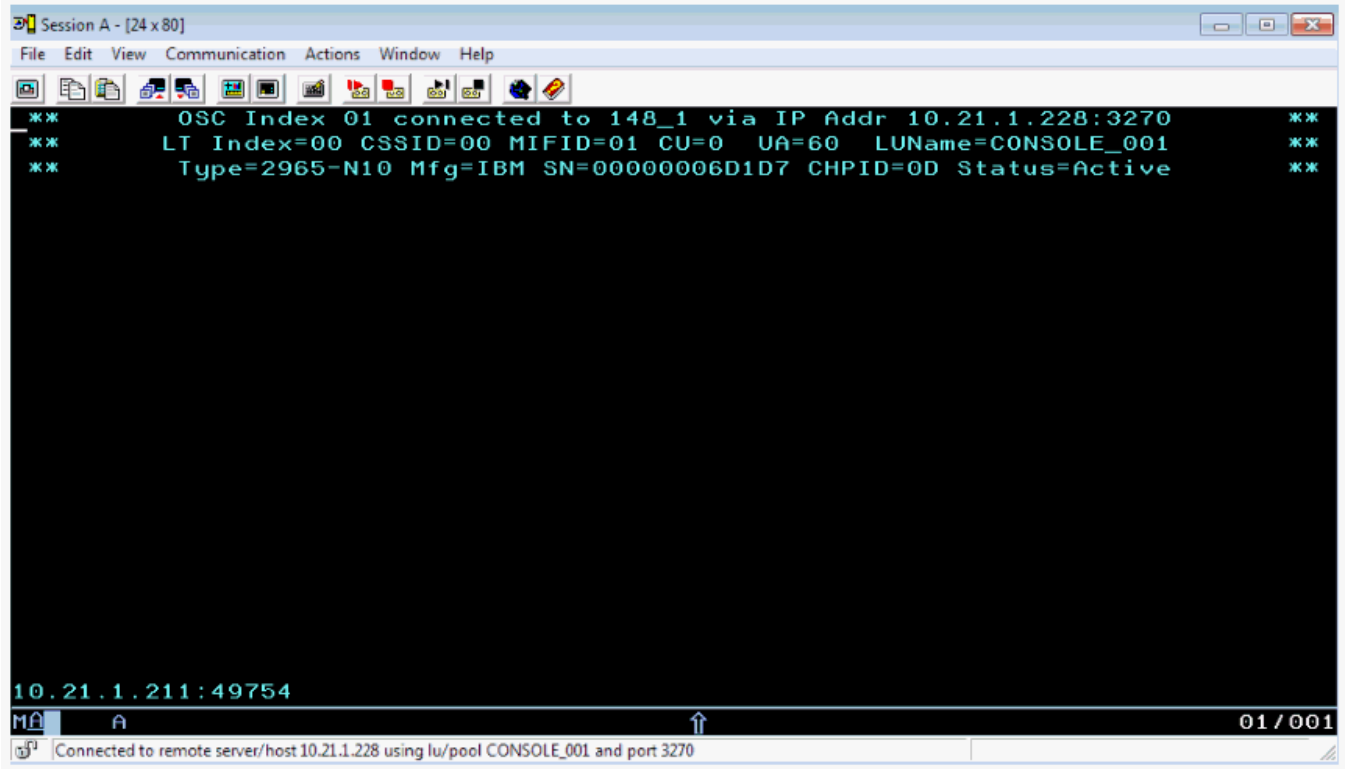



*Figure 59. E - Capture — [24x80]*

Line 1: 148_1 is the defined server name; 10.21.1.228:3270 shows the defined server address and port number.

Line 2: session index; CSS number; MIF ID number, logical CU number (always 0); unit address for this device; LU name.

Line 3: information for the connected processor.

- **Machine Type**: Machine specific

- **Mfg Info**: set to IBM
- **SN**: Serial Number
- **CHPID**: Chpid Number
- **Status**: Active or Inactive – Active denotes LPAR has been activated for this defined connection and is ready to be enabled by the Host Operating System

**Important Note**: 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
UndefinedCode=Y
```

If these statements are 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.

## Defining a secure PCOMM TN3270E session

**About this task**

This procedure involves the following:

1. “Importing self-signed or CA signed certificate ” on page 81
2. “Defining the secure PCOMM TN3270E session” on page 89

### Importing self-signed or CA signed certificate

**About this task**

Start from the Windows desktop - Operating System Level Dependent

**Procedure**

1. Select Programs --> IBM Personal Communications --> Utilities --> Certificate Management

   The IBM Key Management window is displayed.
2. Click the Open icon.

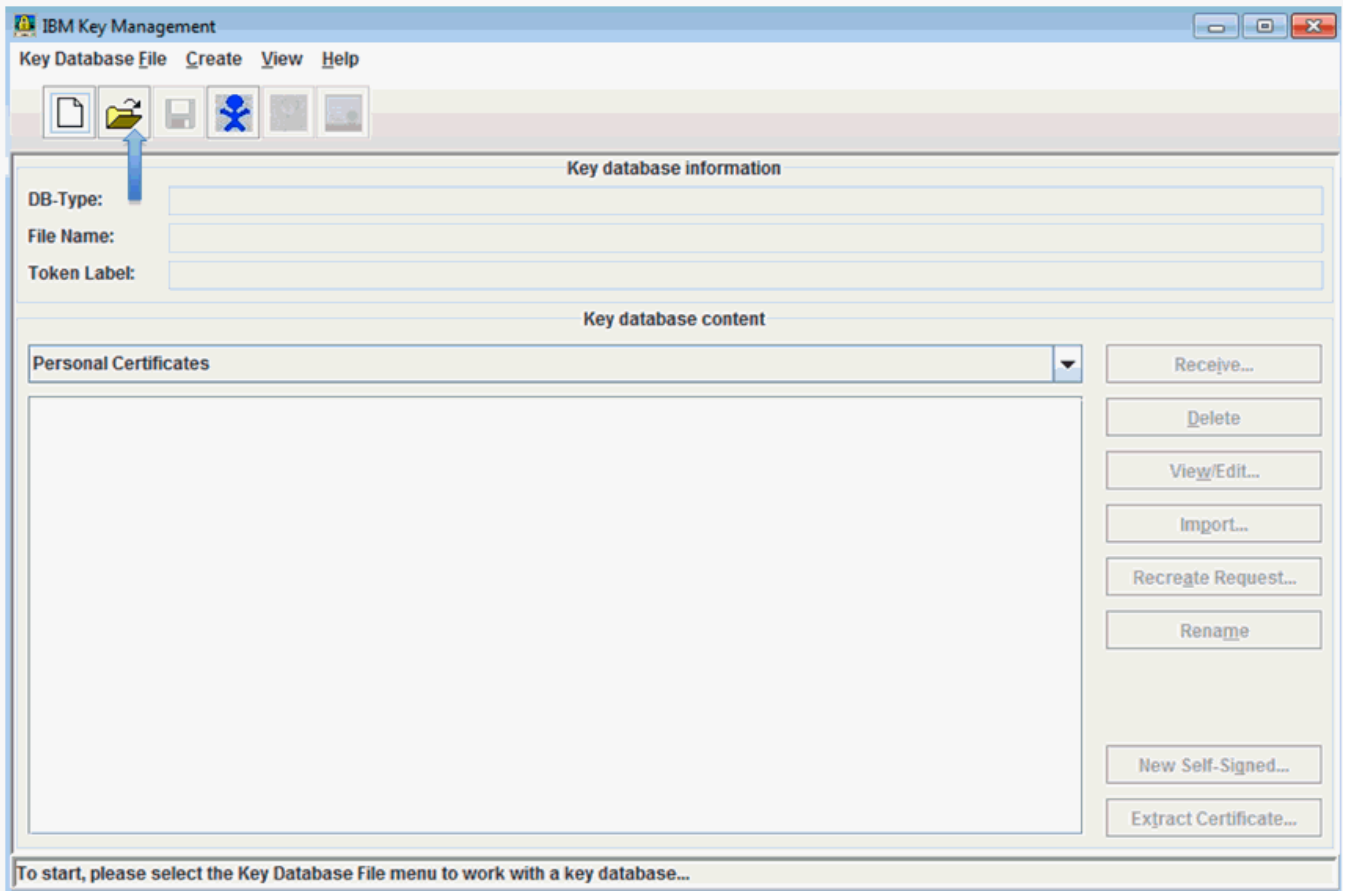



*Figure 60. IBM Key Management, Open icon*

3. From the Open window, click OK

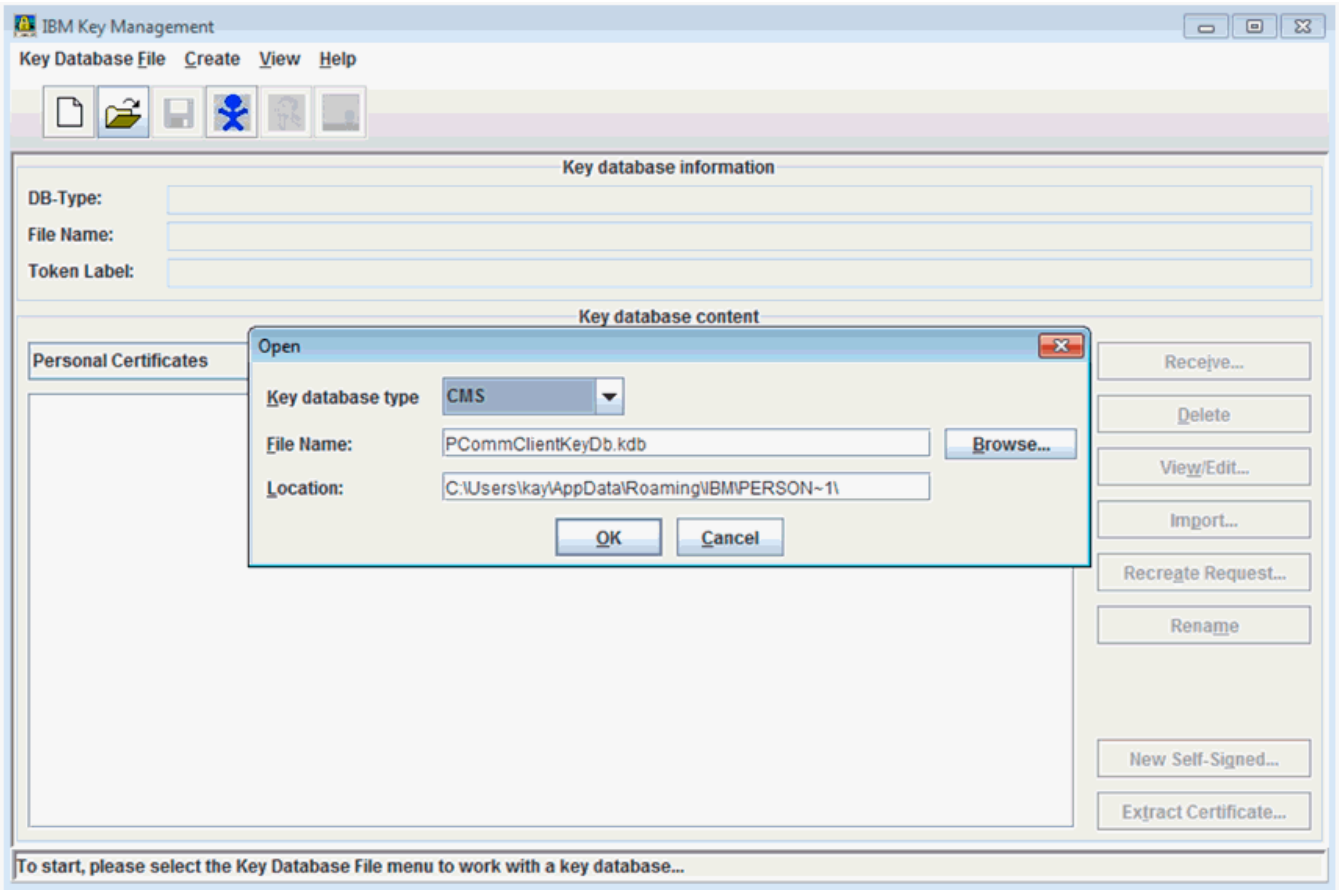



*Figure 61. IBM Key Management, Open window*

4. In the Password Prompt, enter **pcomm**.

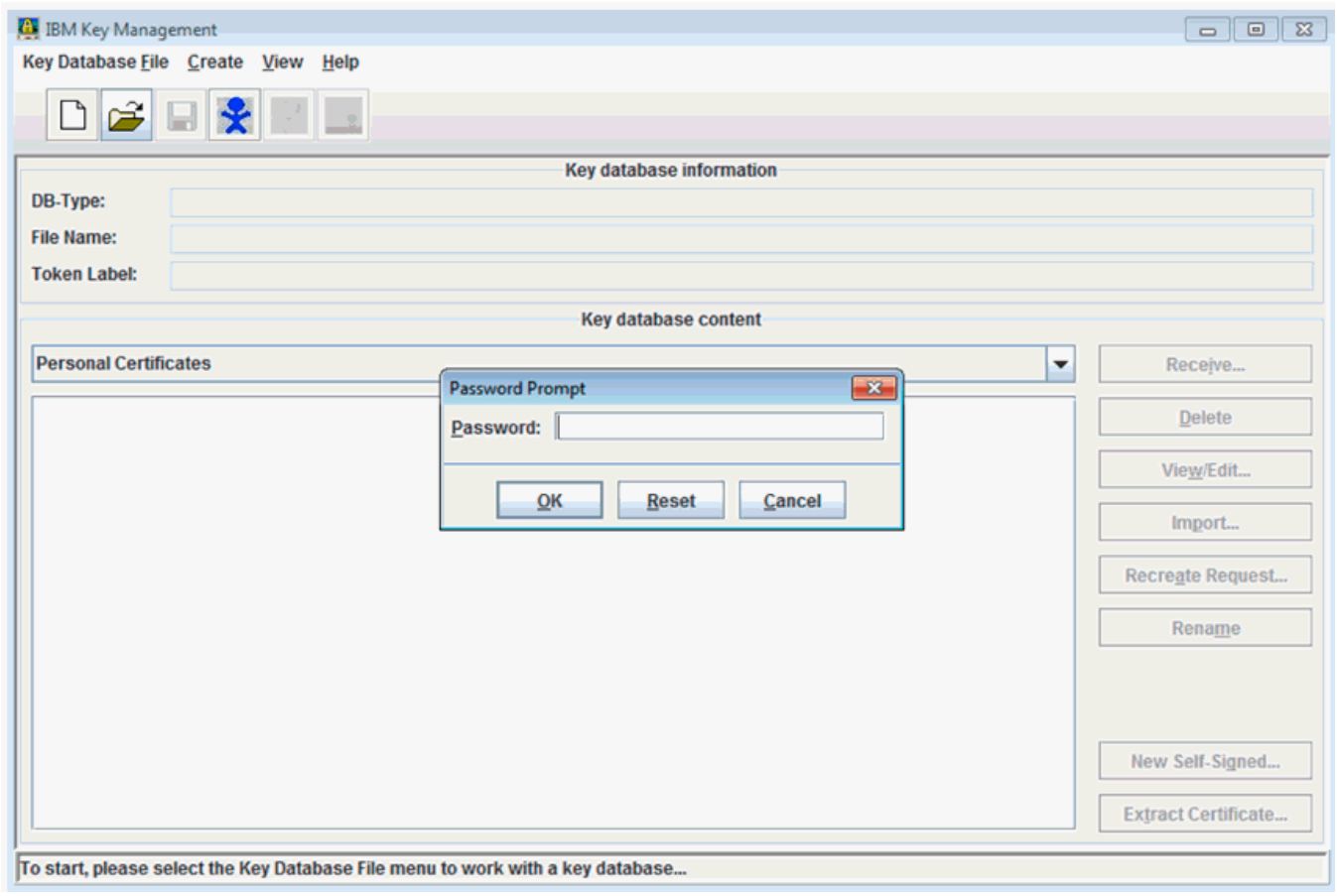



*Figure 62. IBM Key Management, Password Prompt*

5. Click the down arrow under **Key database content** to select the type of certificate and select **Signer Certificates**

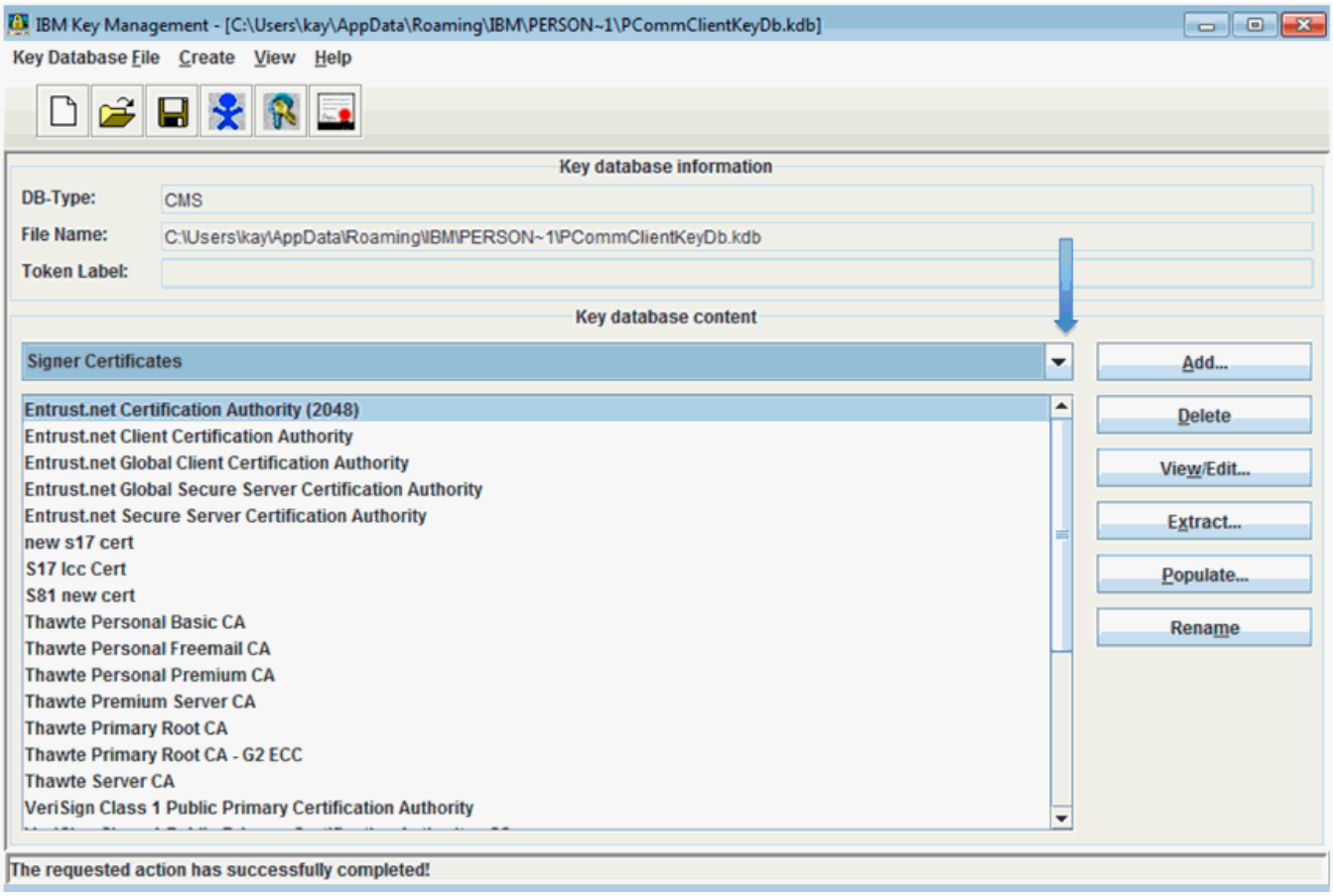



*Figure 63. IBM Key Management, Signer Certificates*

6. Click the Add button

   The Open window is displayed.

7. Enter the filename and location of the signer certificate and click **OK**.

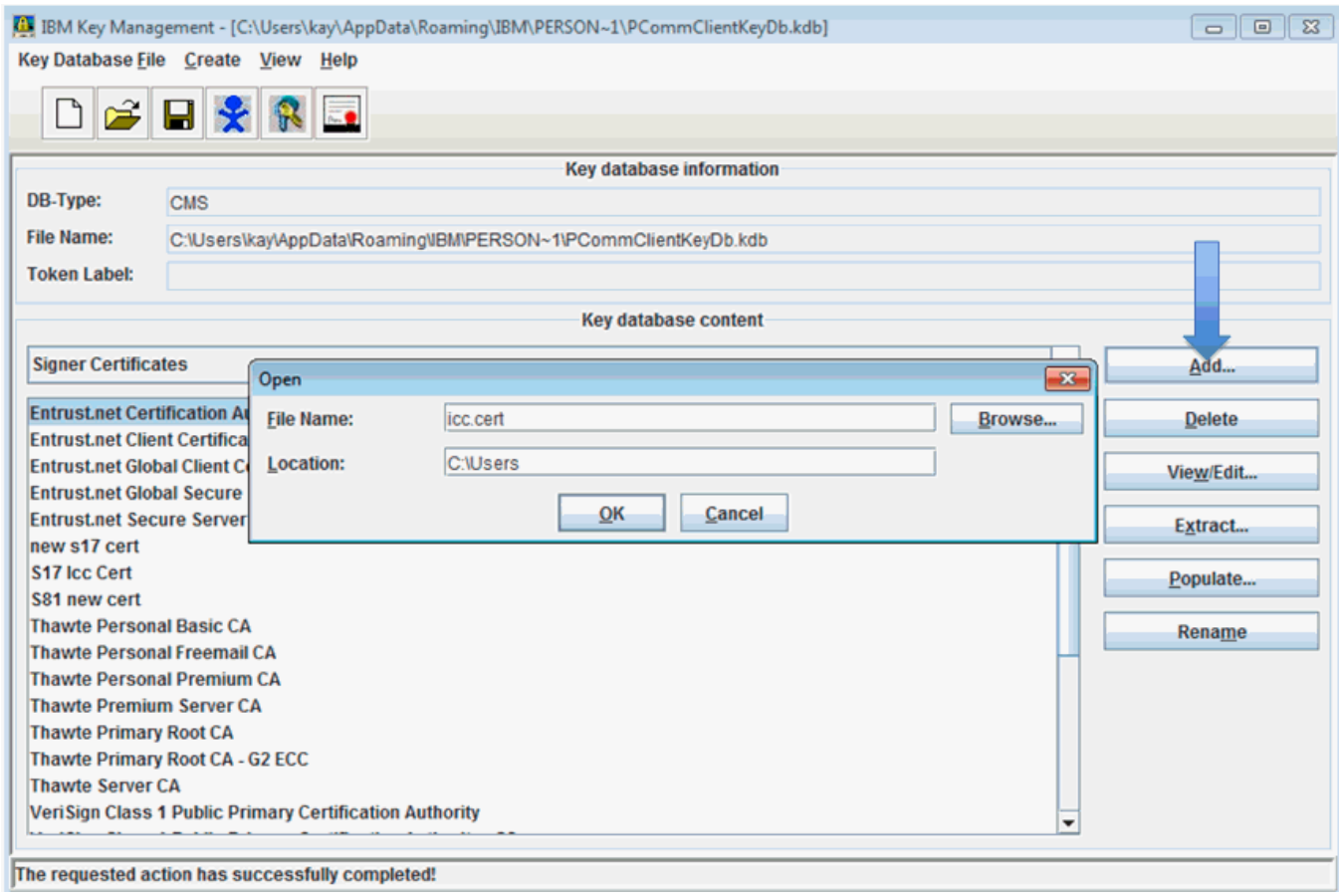



*Figure 64. IBM Key Management, filename and location of signer certificate*

8. From the Enter a Label window, type a name (for example, OSA-ICC Cert) and click **OK**.

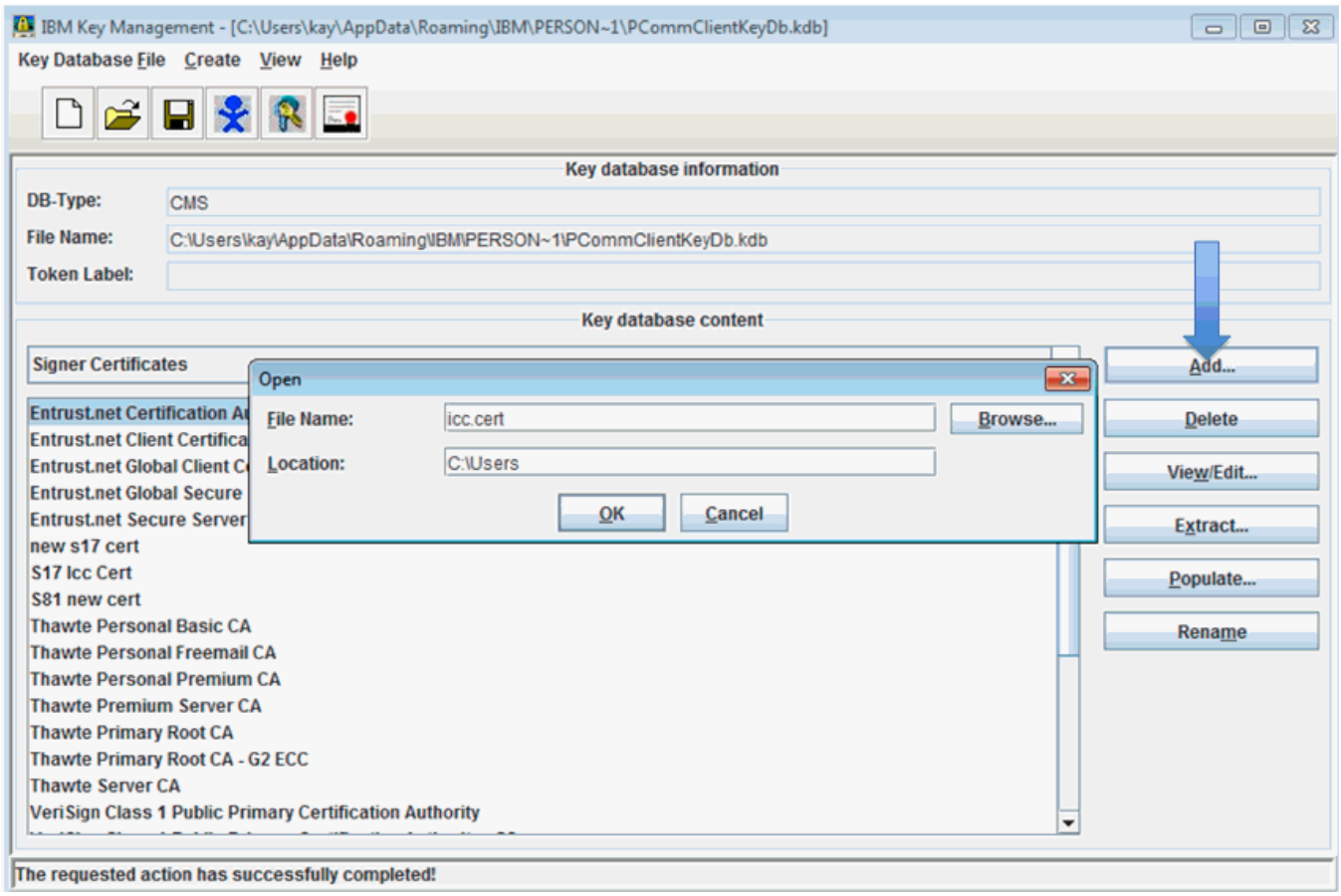



*Figure 65. IBM Key Management, filename and location of signer certificate*

The Name is now in the Key Database Content window and the certificate is ready to use.

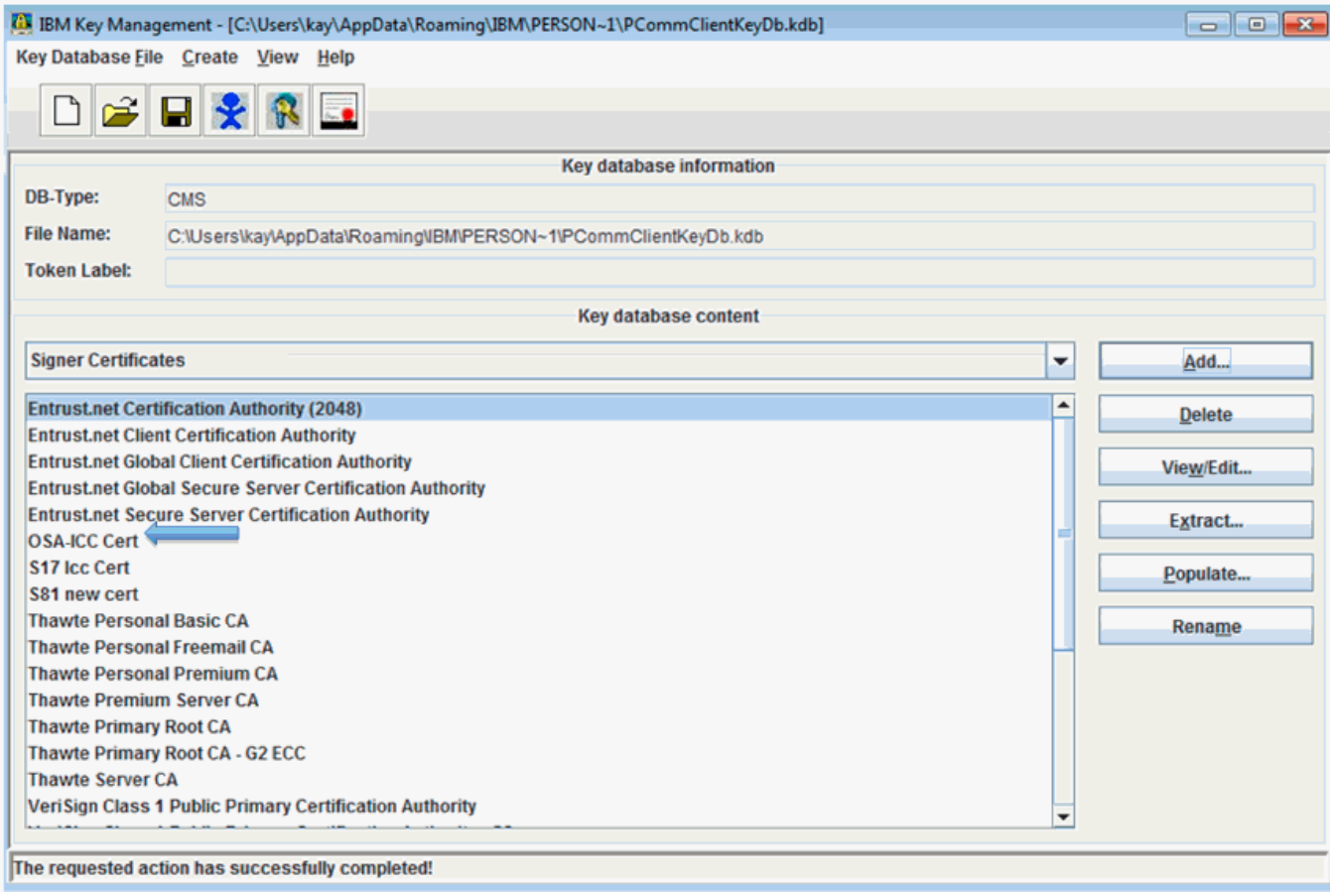



*Figure 66. IBM Key Management, new signer certificate*

**Results**

Session Connected Securely

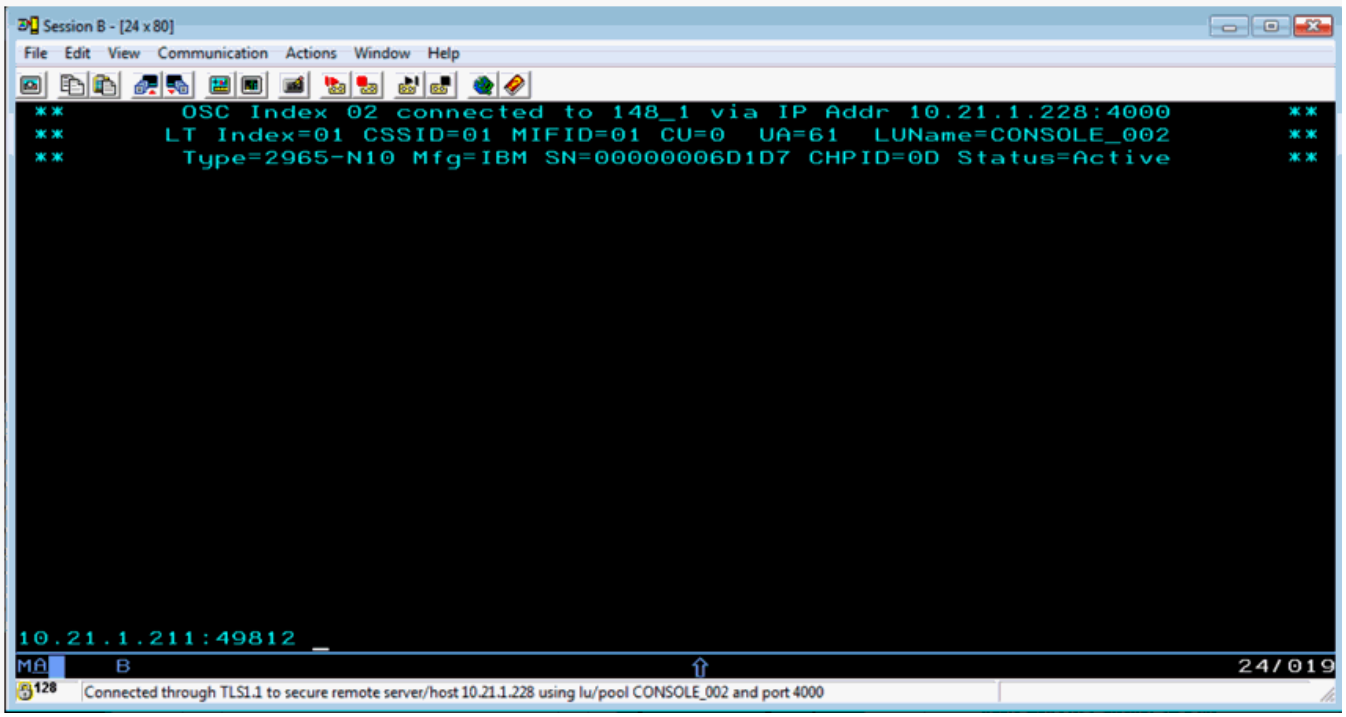



*Figure 67. Section connected securely*

The lock symbol in bottom left hand Status Area indicates a Secure versus Non-Secure Connection.

The Client IP and TCP Port Number are shown on the Console (for example, 10.21.1.211:49812) and matches the information shown on Display Client Connections.

The bottom status line reports Connected through TLS1.1 encryption through Server IP, LU Name and Secure Port Number all set in OSA-ICC Server Configuration.

## Defining the secure PCOMM TN3270E session

### About this task

The initial setup for IP, LU Name, and Port Number is the same as for a non-secure session.

### Procedure

1. Under Link Parameters in the Custom Configuration Options choose the Security Setup Tab.

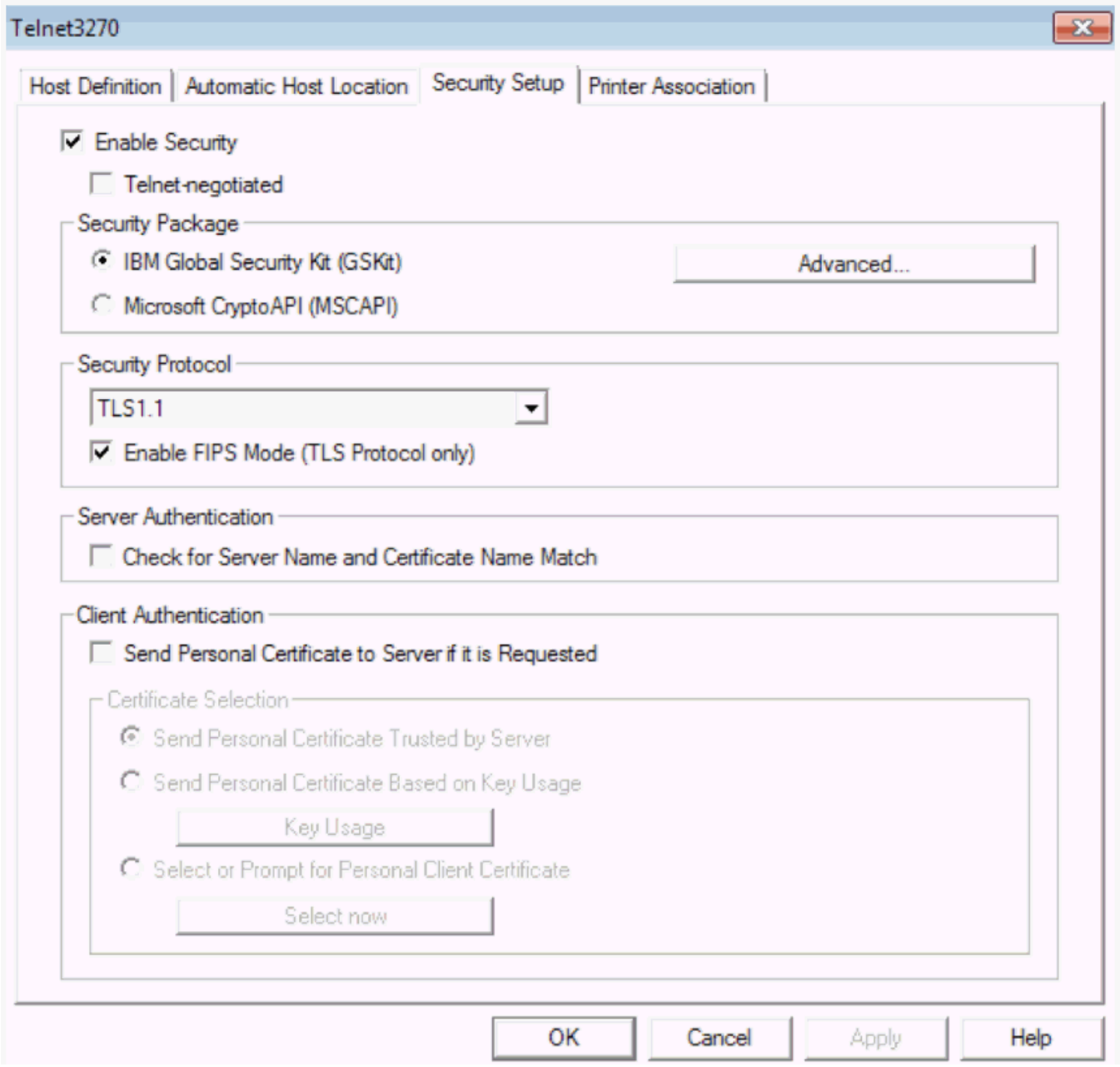



*Figure 68. Custom Configuration Options, Security Setup tab*

2. Click Enable Security
3. Choose your security package.

   This example uses **IBM Global Security Lit (GSKit)**.
4. Select the Security Protocol (TLS 1.1)
5. Select the FIPS mode (Enable)
6. Make sure the following is left unchecked:
   - Telnet negotiated
   - Server Authentication
   - Client Authentication

# Chapter 11. Error and warning messages

New for OSA-ICC for z13 is support to create error and warning messages directly to the iqyylog.

The new tag OsaIccMsg provides a limited set or error and warning messages. The entry provides 8 bytes of information. The first 4 bytes (E191212A in the example), is the SE reference tag and is for information only. The next 4 bytes provide the PCHID number (0148) and the message code. Message details are provided in Table 2 on page 91.

*Table 2. Informational and error messages from OsaIccMsg.* The first three messages in the table are Informational, while the final three are Errors.

| Tag | Meaning |
|---|---|
| 0x1001 | Informational: The TLS files were created on the SE Disk by this PCHID |
| 0x1002 | Informational: The key and certificates were regenerated by this PCHID |
| 0x1003 | Informational: The key and certificates files were added to this PCHID configuration file |
| 0xE001 | Error: No Hut File (temporary Configuration file) present on the SE Disk |
| 0xE002 | Error: Bad Hul File (Configuration File) present on the SE Disk |
| 0xE003 | Error: No Hul File (Configuration File) present on the SE Disk |

By validating your configuration file, either by the ***Validate panel values*** window or the ***Validate Source File*** window, 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*** window or in the source file as comments. Table 3 on page 91 is a list of errors and warnings that you could receive. Note that Errors (1000 and up) must be corrected before attempting to activate a configuration.

*Table 3. 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 |

| *Table 3. Errors from validate source file (continued)* | |
|---|---|
| **Code** | **Text** |
| 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 |
| 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 |

| *Table 3. Errors from validate source file (continued)* | |
|---|---|
| **Code** | **Text** |
| 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 |
| 1065 | // @@@ error: No value for TLS protocol version |
| 1067 | // @@@ error: No value for HOST_LL_ADDRESS/ PREFIX, must be auto generated link local address |
| 1068 | // @@@ error: No value for ADDR_TYPE, use LINK_LOCAL or STATIC keyword |
| 1069 | // @@@ error: No value for HOST_IPV6_ADDRESS/ PREFIX, expects link local or static ipv6 address |
| 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 |
| 1084 | // @@@ error: Have to define host Ethernet standard between <OSC_PHYSICAL_PORT#> and </OSC_PHYSICAL_PORT#> tags |
| 1086 | // @@@ error: No value for Auto generated Link Local address |
| 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 |

| *Table 3. Errors from validate source file (continued)* | |
|---|---|
| **Code** | **Text** |
| 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 |
| 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 |

| *Table 3. Errors from validate source file (continued)* | |
|---|---|
| **Code** | **Text** |
| 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 |
| 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 |

| *Table 3. Errors from validate source file (continued)* | |
|---|---|
| **Code** | **Text** |
| 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 |
| 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. |

| *Table 3. Errors from validate source file (continued)* | |
|---|---|
| **Code** | **Text** |
| 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 |
| 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 |

*Table 3. Errors from validate source file (continued)*

| Code | Text |
|---|---|
| 1317 | // @@@ error: Physical port # has to be a decimal number |
| 1318 | // @@@ error: Missing <OSC_PHYSICAL_PORT#> tag |
| 1933 | // @@@ error: No Valid Port number specified |
| 1934 | // @@@ error: IPV4 Secure Port matches NonSecure port number |
| 1952 | // @@@ error: IPV4 Out of range port value |
| 1955 | // @@@ error: IPV4 Host Secure port value used for previous physical Secure port definition |
| 5056 | // @@@ error: Invalid TLS Version |
| 5059 | // @@@ error: IPV6 Host port value used for previous physical port definition |
| 5060 | // @@@ error: IPV6 Out of range port value |
| 5061 | // @@@ error: IPV6 Host Secure port value used for previous physical Secure port |
| 5062 | // @@@ error: IPV6 Out of range secure port value |
| 5064 | // @@@ error: IPV6 Host/Link LL IP value used for previous physical port definition |
| 5065 | // @@@ error: IPV6 Host IP value is in bad format |
| 5066 | // @@@ error: IPV6 Have to have a least one non-zero port between <OSC_PHSYICAL_PORT#> and </OSC_PHYSICAL_PORT#> tags |
| 5067 | // @@@ error: IPV6 prefix value is out of range[1-128] |
| 5068 | // @@@ error: IPV6 Secure Port matches NonSecure port number |
| 5069 | // @@@ error: IPV6 port numbers matches to ipv4 |
| 6061 | // @@@ error: Invalid IPV6 address type string |
| 6062 | // @@@ error: Missing HOST IPV6 PREFIX |
| 6063 | // @@@ error: Missing IPV6 Link Local PREFIX |
| 6066 | // @@@ error: Bad IPv6 syntax format missing slash / |
| 6067 | // @@@ error: Bad IPv6 syntax format - invalid prefix value after / |
| 6068 | // @@@ error: Link local address is not same as Auto generated on |
| 6069 | // @@@ error: Invalid IPV6 Address / is not correct |
| 6070 | // @@@ error: Invalid Link Local IPV6 Address |

| *Table 3. Errors from validate source file (continued)* | |
|---|---|
| **Code** | **Text** |
| 6071 | // @@@ error: HOST IPV6 address and Address type are not matching |
| 6072 | // @@@ error: Writing subnet mask Exception Error |
| 6073 | // @@@ error: Invalid IPV4 prefix value |
| 6074 | // @@@ error: IPV6 HOST address is not valid for NONE cfg |
| 6075 | // @@@ error: IPV6 Have to have a least one non-zero port between <OSC_PHSYICAL_PORT#> and |
| 6076 | // @@@ error: IPV6 default gateway address[All Zeros] is not valid for the STATIC |
| 6077 | // @@@ error: Invalid IPV6 address |
| 6078 | // @@@ error: Port is defined but IPV4 Host IP value is in bad format |
| 6079 | // @@@ error: Secure Port is defined but IPV4 Host IP value is in bad format |
| 6080 | // @@@ error: IPV6 address is in bad format missing /prefix |
| 6081 | // @@@ error: Configured HOST IPV6 address/ prefix is not same as auto generated |
| 6082 | // @@@ error: Missing IPV4 prefix or subnet value |
| 6083 | // @@@ error: Configuring Link Local prefix is not valid while Link is down |
| 6084 | // @@@ error: Configuring Link Local IPV6 address is not valid while Link is down |
| 6085 | // @@@ error: Configuring IPv4 is not valid while Link is down |
| 6086 | // @@@ error: Bad IPv6 syntax format |

| *Table 4. 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 5. Errors from validate windows* | |
|---|---|
| **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. |
| 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. |

| *Table 5. Errors from validate windows (continued)* | |
|---|---|
| **Code** | **Text** |
| 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 |
| 1992 | // @@@ Error There is no HUL or HUT present or with zero size |

| *Table 6. Warnings from validate windows* | |
|---|---|
| **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 |
| 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 |

## Debugging tips

New for OSA-ICC for z13 is support to create error and warning messages directly to the iqyylog.

1. Update the config trm with the required IPv4 subnet mask and ICC calculates the prefix and populates into server configuration panel. From the GA2 driver onwards, server configuration panel expects CIDR representation of IPv4 address.
2. Link local IPv6 address will not be populated if the interface is not wired; that is, it will be blank.
3. Execute the **osass** command to see the list of TCP/IP listen servers opened on the given server configuration and list of network sessions connected to PCHID with the current state.
4. From z14 GA2 and beyond, hardware configuration changing from 3270 to 3215 (and from 3215 to 3270):
   - Need to perform "Reset To Defaults" after backing up the old config source trm file.
   - After reset to factory settings - reload/validate and activate the backup config source trm file.

5. For SSL certificates, always check the "certificate scope[Shared or Individual]" and "certificate type" on the Manage Security certificates to understand the active certificate on the PCHID.
6. Imported certificate fail or success can be verified by looking at the following sock master HYDRA INFO traces:
   - ERR_USER_CERT_IMPORT - importing certificate is failed
   - SUCCESS_USER_CERT_IMPORT - certificate import went successful

The following are problem determination tips on connection to client sessions.

1. Use the View Port Parameter (see “View port parameters” on page 17) to check if the OSA port 0/1 has a good network connection:
   a. Active speed, mode: 1000Mb or 100Mb, Full duplex
   b. An "Unknown" connection means a lost network connection; get your network administrator to help. Total packets Transmitted/Received counts should be increasing between each display.
2. Use the Debug utilities in Chapter 7, “Debug utilities,” on page 49
   a. Use the PING utility to PING the gateway and client session IP addresses.
   b. PING passed between the client and OSA, but still unable to establish connections.
   c. Manually take the trace and log for IBM Support.
   d. Pick the card trace/log/dump facilities (see “OSA-ICC configuration and debug windows” on page 13) on the OSA-ICC PCHID. Do the Read Trace Buffer and follow by the Read Log Buffer option (concurrent).
3. Send the trace and log to IBM, as follows:
   a. On the HMC/Tasks Index and pick the Transmit Service Data, Select the CEC.
   b. Pick Support System for sending the log to IBM
   c. Pick Hydra service data for the OSA trace/log data.
4. Choose Send to send the data
   a. Open a problem record on HMC
   b. On the HMC/Tasks Index and pick Report a Problem, select the CEC
   c. Pick I/O option
5. Additional information to be mentioned:
   a. Failing OSA-ICC PCHID number
   b. Which LPAR image or images were having problems
   c. Any problem determination was done, if Read Trace/Log Buffer were collected during the error condition.

# Appendix A. ASCII table

| Char | Dec | Oct | Hex | Char | Dec | Oct | Hex | Char | Dec | Oct | Hex |
|---|---|---|---|---|---|---|---|---|---|---|---|
| (sp) | 32 | 0040 | 0x20 | @ | 64 | 0100 | 0x40 | ` | 96 | 0140 | 0x60 |
| ! | 33 | 0041 | 0x21 | A | 65 | 0101 | 0x41 | a | 97 | 0141 | 0x61 |
| " | 34 | 0042 | 0x22 | B | 66 | 0102 | 0x42 | b | 98 | 0142 | 0x62 |
| # | 35 | 0043 | 0x23 | C | 67 | 0103 | 0x43 | c | 99 | 0143 | 0x63 |
| $ | 36 | 0044 | 0x24 | D | 68 | 0104 | 0x44 | d | 100 | 0144 | 0x64 |
| % | 37 | 0045 | 0x25 | E | 69 | 0105 | 0x45 | e | 101 | 0145 | 0x65 |
| & | 38 | 0046 | 0x26 | F | 70 | 0106 | 0x46 | f | 102 | 0146 | 0x66 |
| ' | 39 | 0047 | 0x27 | G | 71 | 0107 | 0x47 | g | 103 | 0147 | 0x67 |
| ( | 40 | 0050 | 0x28 | H | 72 | 0110 | 0x48 | h | 104 | 0150 | 0x68 |
| ) | 41 | 0051 | 0x29 | I | 73 | 0111 | 0x49 | i | 105 | 0151 | 0x69 |
| * | 42 | 0052 | 0x2a | J | 74 | 0112 | 0x4a | j | 106 | 0152 | 0x6a |
| + | 43 | 0053 | 0x2b | K | 75 | 0113 | 0x4b | k | 107 | 0153 | 0x6b |
| , | 44 | 0054 | 0x2c | L | 76 | 0114 | 0x4c | l | 108 | 0154 | 0x6c |
| - | 45 | 0055 | 0x2d | M | 77 | 0115 | 0x4d | m | 109 | 0155 | 0x6d |
| . | 46 | 0056 | 0x2e | N | 78 | 0116 | 0x4e | n | 110 | 0156 | 0x6e |
| / | 47 | 0057 | 0x2f | O | 79 | 0117 | 0x4f | o | 111 | 0157 | 0x6f |
| 0 | 48 | 0060 | 0x30 | P | 80 | 0120 | 0x50 | p | 112 | 0160 | 0x70 |
| 1 | 49 | 0061 | 0x31 | Q | 81 | 0121 | 0x51 | q | 113 | 0161 | 0x71 |
| 2 | 50 | 0062 | 0x32 | R | 82 | 0122 | 0x52 | r | 114 | 0162 | 0x72 |
| 3 | 51 | 0063 | 0x33 | S | 83 | 0123 | 0x53 | s | 115 | 0163 | 0x73 |
| 4 | 52 | 0064 | 0x34 | T | 84 | 0124 | 0x54 | t | 116 | 0164 | 0x74 |
| 5 | 53 | 0065 | 0x35 | U | 85 | 0125 | 0x55 | u | 117 | 0165 | 0x75 |
| 6 | 54 | 0066 | 0x36 | V | 86 | 0126 | 0x56 | v | 118 | 0166 | 0x76 |
| 7 | 55 | 0067 | 0x37 | W | 87 | 0127 | 0x57 | w | 119 | 0167 | 0x77 |
| 8 | 56 | 0070 | 0x38 | X | 88 | 0130 | 0x58 | x | 120 | 0170 | 0x78 |
| 9 | 57 | 0071 | 0x39 | Y | 89 | 0131 | 0x59 | y | 121 | 0171 | 0x79 |
| : | 58 | 0072 | 0x3a | Z | 90 | 0132 | 0x5a | z | 122 | 0172 | 0x7a |
| ; | 59 | 0073 | 0x3b | [ | 91 | 0133 | 0x5b | { | 123 | 0173 | 0x7b |
| < | 60 | 0074 | 0x3c | \ | 92 | 0134 | 0x5c | \| | 124 | 0174 | 0x7c |
| = | 61 | 0075 | 0x3d | ] | 93 | 0135 | 0x5d | } | 125 | 0175 | 0x7d |
| > | 62 | 0076 | 0x3e | ^ | 94 | 0136 | 0x5e | ~ | 126 | 0176 | 0x7e |
| ? | 63 | 0077 | 0x3f | _ | 95 | 0137 | 0x5f | | | | |

*Figure 69. Network topology Diagram 1*

# Appendix B. Sample signed certificates

## Sample certificate signing request

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: CN=OsaIccTLSServer
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c1:bb:47:cb:de:77:22:59:51:5b:3e:4e:f1:db:
                    9b:14:5a:b7:42:ef:51:78:e2:b4:c5:73:1a:c7:93:
                    36:6d:5c:28:4f:dd:ef:ea:e5:60:ac:00:aa:ff:35:
                    60:f6:05:1a:0b:30:14:5b:df:7b:0e:23:33:86:1d:
                    16:0c:65:bd:7e:7c:32:e1:d4:95:51:e5:3e:c6:1b:
                    6c:c8:7a:17:d0:c4:d7:4b:67:62:8a:52:6a:e0:78:
                    ce:b4:14:97:9f:a4:63:87:5b:36:d9:ab:d9:ac:30:
                    7e:55:32:a1:ed:01:2e:e4:e9:92:a2:d0:00:b1:16:
                    91:56:2f:6f:5c:5d:72:9f:5e:98:f5:dd:a3:bc:d5:
                    c2:3a:18:7d:bf:f4:88:f7:a1:c7:ec:78:30:a5:4c:
                    09:9b:69:c5:af:ff:b5:d0:5c:b4:11:95:02:76:67:
                    7e:84:b9:55:67:18:46:43:0c:55:67:40:dc:1c:92:
                    36:3d:68:51:01:14:b7:83:04:cb:cb:3f:f3:8c:de:
                    23:31:d8:a7:16:de:21:fb:1d:46:07:da:23:82:5c:
                    2a:b0:e3:f5:49:fb:ee:ba:a7:a2:3d:cf:f6:1d:7c:
                    46:16:c8:cf:39:da:10:0c:d8:70:14:db:6f:52:c3:
                    89:7c:09:51:6b:20:ed:1a:b8:54:43:f4:ce:82:7e:
                    a9:5b
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         46:18:6e:f3:69:3e:2a:08:9d:a3:07:a9:cf:d3:bd:bd:79:7b:
         25:ef:3f:8f:ba:24:f6:fb:64:3f:19:d6:d2:bf:58:bd:75:1c:
         b5:66:4f:e1:a9:e5:e3:0b:e8:4d:cf:25:d5:13:0c:11:df:48:
         da:10:bb:3c:68:28:0a:f0:8b:e2:80:5e:0d:42:da:2d:8c:11:
         8d:5b:62:6d:06:cf:83:81:9b:36:7a:dd:43:43:33:64:bf:e5:
         7c:33:21:51:e2:46:01:09:16:f6:9a:dd:c5:d5:c5:2a:08:ef:
         b1:2d:e4:26:8d:99:ab:93:c7:73:49:3c:1a:d5:ae:0b:d4:70:
         a1:b4:9f:2f:9e:4a:34:fb:b9:e3:c1:85:41:04:ae:91:39:d1:
         a9:e0:1c:8c:6e:c8:12:01:3c:1a:67:6e:5c:2e:c3:58:93:43:
         18:ab:f0:5a:3b:a1:f4:e9:22:6d:7a:ef:d3:e6:4a:65:6d:0c:
         1b:c2:dc:e6:d0:63:d7:93:b8:6c:d0:00:7c:6b:7a:20:f2:26:
         5e:f0:57:fd:c4:56:56:c5:de:eb:0b:bc:24:a6:c2:61:ee:4b:
         0e:c6:3e:23:46:3c:17:fe:0e:ae:92:9d:5e:49:86:e0:6d:4d:
         94:99:31:be:9b:ba:e6:3b:44:83:13:33:88:a1:02:b2:70:19:
         3d:f0:dc:da
```

## Sample self-signed certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            da:50:cb:99:52:41:22:88
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=OsaIccTLSServer
        Validity
            Not Before: Jan 29 16:51:44 2016 GMT
            Not After : Jan 28 16:51:44 2019 GMT
        Subject: CN=OsaIccTLSServer
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c1:bb:47:cb:de:77:22:59:51:5b:3e:4e:f1:db:
                    9b:14:5a:b7:42:ef:51:78:e2:b4:c5:73:1a:c7:93:
```

```
                    36:6d:5c:28:4f:dd:ef:ea:e5:60:ac:00:aa:ff:35:
                    60:f6:05:1a:0b:30:14:5b:df:7b:0e:23:33:86:1d:
                    16:0c:65:bd:7e:7c:32:e1:d4:95:51:e5:3e:c6:1b:
                    6c:c8:7a:17:d0:c4:d7:4b:67:62:8a:52:6a:e0:78:
                    ce:b4:14:97:9f:a4:63:87:5b:36:d9:ab:d9:ac:30:
                    7e:55:32:a1:ed:01:2e:e4:e9:92:a2:d0:00:b1:16:
                    91:56:2f:6f:5c:5d:72:9f:5e:98:f5:dd:a3:bc:d5:
                    c2:3a:18:7d:bf:f4:88:f7:a1:c7:ec:78:30:a5:4c:
                    09:9b:69:c5:af:ff:b5:d0:5c:b4:11:95:02:76:67:
                    7e:84:b9:55:67:18:46:43:0c:55:67:40:dc:1c:92:
                    36:3d:68:51:01:14:b7:83:04:cb:cb:3f:f3:8c:de:
                    23:31:d8:a7:16:de:21:fb:1d:46:07:da:23:82:5c:
                    2a:b0:e3:f5:49:fb:ee:ba:a7:a2:3d:cf:f6:1d:7c:
                    46:16:c8:cf:39:da:10:0c:d8:70:14:db:6f:52:c3:
                    89:7c:09:51:6b:20:ed:1a:b8:54:43:f4:ce:82:7e:
                    a9:5b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                4E:9E:53:8E:2E:0F:2B:04:CC:C4:EB:B4:41:FC:B0:67:5C:E0:6E:B8
            X509v3 Authority Key Identifier:
                keyid:4E:9E:53:8E:2E:0F:2B:04:CC:C4:EB:B4:41:FC:B0:67:5C:E0:6E:B8
```

```
            X509v3 Basic Constraints:
                CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
         23:ee:f7:02:fe:48:92:0e:8f:df:36:bc:c2:16:e6:b2:e4:a4:
         75:67:d5:f5:74:c9:eb:91:76:d7:d0:b0:44:f6:58:ac:1b:a8:
         40:6b:34:31:8b:75:a5:cb:75:ae:1b:4b:e9:ee:80:54:8b:57:
         d2:aa:7b:a8:0a:66:2e:8e:3b:a6:46:5d:0a:ea:c2:69:68:62:
         56:53:74:83:e4:a5:79:ec:e3:ae:e9:ab:54:9c:c2:60:05:f5:
         04:02:99:57:73:81:5b:6e:6b:cf:72:47:63:7d:be:51:fd:a0:
         2c:5a:59:80:bc:00:23:25:fa:74:39:2c:7b:c1:34:c4:57:e5:
         43:f4:33:2a:d6:11:7c:8d:5a:8e:77:f4:bc:41:04:c9:0d:9d:
         6e:8a:be:65:f4:2d:e7:7a:29:5c:cc:c8:e5:a9:3d:55:d7:35:
         b4:5e:cf:01:4c:58:2f:e5:df:b4:4c:a0:b5:e1:b2:a8:89:8a:
         0a:44:3d:bb:ff:22:9c:a9:70:a7:54:30:1a:bd:ae:ca:08:fb:
         4f:05:0d:d5:7a:bf:03:8f:6f:ae:ed:08:2f:f1:e6:dc:10:ae:
         4e:a8:12:76:05:60:b3:be:8f:14:55:21:a9:bd:fe:39:84:c0:
         16:7c:53:69:92:07:67:ab:5d:9c:59:bd:47:02:55:2c:f0:18:
         69:c3:14:21
```

# Appendix C. Network topology

The OSA-ICC adapter supports two physical ports for each pchid. The server definition for each physical port defines a unique secure and/or non-secure TCP port number, IP address and subnet. These server definitions allow for an isolated Local Area Network (LAN) to be created for each physical port. Any external network traffic is routed through a common default gateway defined for both ports. An example illustrating an OSA-ICC multi-port connection is given in the network topology diagram in Figure 70 on page 107.

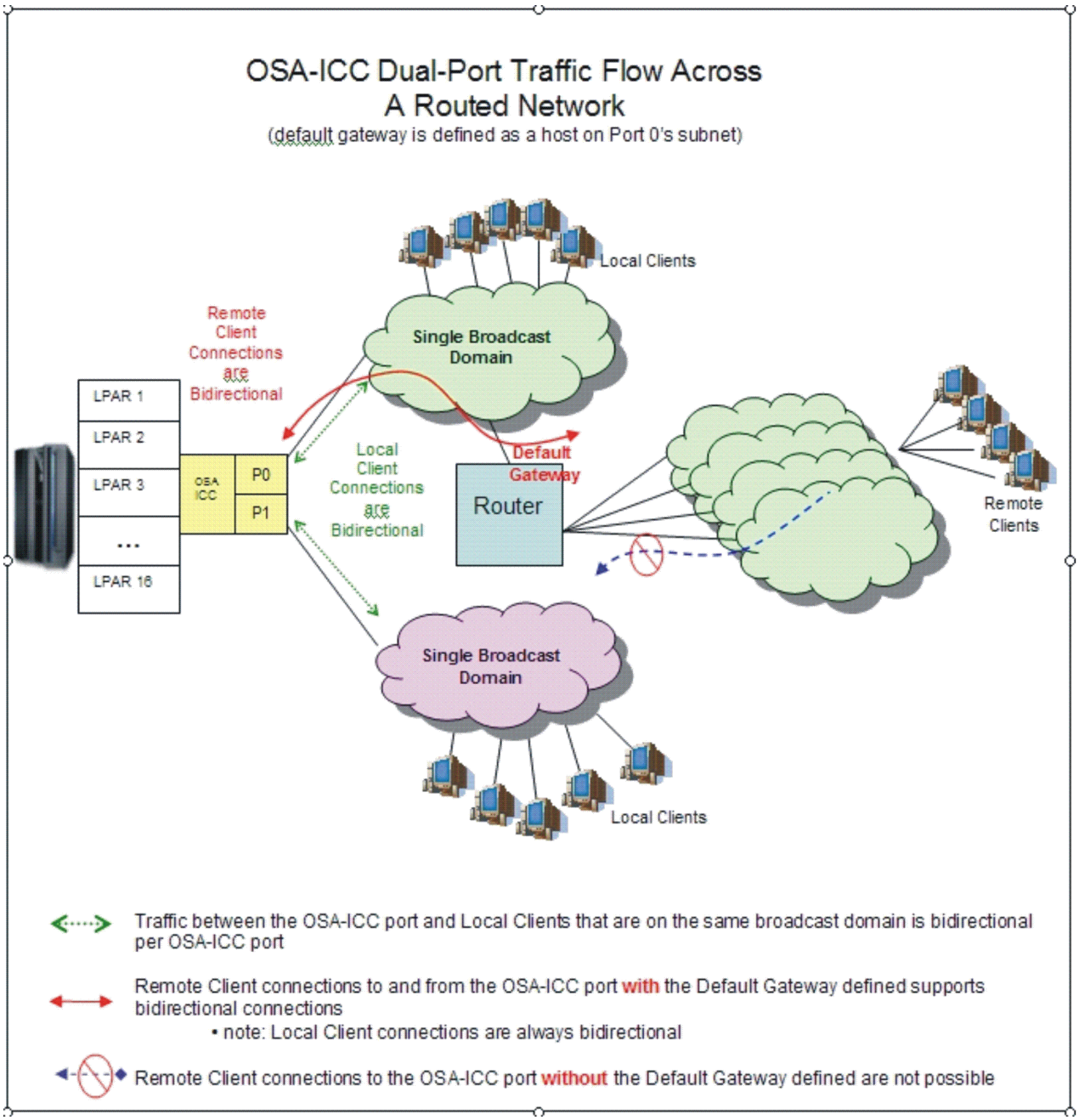



*Figure 70. Network topology diagram*

Figure 70 on page 107 shows connectivity to an ICC adapter 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 external network traffic is only allowed to travel in one direction through P0 because the local clients reside on the same subnet as the default gateway. The clients connected to P1 are restricted to communicate only with the clients of that subnet.

# 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.*

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

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 Copyright and Trademark information (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

SC27-9003-02