mTera Provisioning User’s Guide

76.MTFP10/15

mTera™ Universal Transport Platform

7190 Element Management System
7194 Network Management System
7191 Craft Station

Revision A, 6/14

FCC Notification Statement

Federal Communications Commission (FCC) Rules require that you be notified of the following:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications not expressly approved by Tellabs Operations, Inc., in writing can void the user’s authority to operate the equipment.

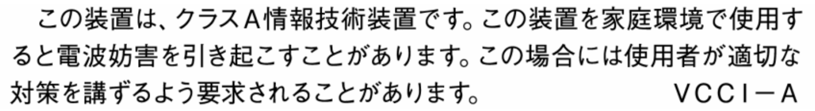
Industry Canada Notification Statement

Industry Canada interference-causing equipment regulations require that you be notified of the following:

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Voluntary Control Council for Interference (VCCI)



この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　VCCI－A

Corporate References

Tellabs and Coriant are joining forces. You may see references to Coriant or Tellabs when doing business with us. Contact information is available at http://www.coriant.com.

Copyright Statement

This manual is protected by U.S. and international copyright laws, conventions, and treaties. Your right to use this manual is subject to limitations and restrictions imposed by applicable licenses and copyright laws. Unauthorized reproduction, modification, distribution, display or other use of this manual may result in criminal and civil penalties.

Trademark Notice

The following trademarks and service marks are owned by Tellabs Operations, Inc., or its affiliates in the United States and/or other countries: BROADLEAF®, CABLESPAN®, CORIANT™, CORIANT DYNAMIC OPTICAL CLOUD™, DXX®, DXX®, DYNAMIC SIGNAL TRANSFER™, FOCUS™, INSIGHT ANALYTICS™, MARTIS®, Martis®, MARTISDXX®, MARTISDXX®, METROCARE℠, METROWATCH®, MTERA™, SILVX®, SILVX INSIGHT®, SILVXMANAGER®, SILVXOSS®, SILVXSOURCE®, SMARTCORE®, SOLAR®, SYCAMORE NETWORKS®, TECHNOLOGY THAT TRANSFORMS THE WAY THE WORLD COMMUNICATES™, T®, TELLABS®, tellabs®, TELLABS PROPARTNER™, TELLABS. THE FUTURE OF YOUR BUSINESS. STARTING NOW™, THE WORLD COMMUNICATES THROUGH TELLABS™, TITAN®, YOUR NETWORKING PARTNER®, XIEON NETWORKS™

Any other company or product names may be trademarks of their respective companies.

Contents Page

Section 1 Introduction 15-1

Section 2 Installing the Craft Station 15-2

Section 3 Commissioning an NE 15-11

Section 4 Navigating the Craft Station 15-25

Section 5 User and Session Management 15-33

Contents **Page**

Contents Page

Contents Page

Contents Page

Section 10 Provisioning Facilities 15-188

Section 11 Provisioning Cross-Connects 15-225

Contents Page

1.Introduction

1.1 The *7191 Craft Station User's Guide* describes network element (NE) turn-up and equipment provisioning of an mTera™ Universal Transport Platform (UTP) using the 7191 Craft Station interface. Access the Craft Station by installing software on a Windows-based PC or laptop.

1.2 Coriant designed the Craft Station to be installed on a laptop computer for direct connection to NEs. Use the Craft Station for routine maintenance, initial turn-up, and provisioning of individual NEs. The Craft Station provides a user-friendly graphical interface in place of TL1 line-interface commands or the complexities of the 7190 Element Management System and the 7194 Network Management System.

Reason for Issue

1.03 Coriant issues this manual at Revision A to include the changes in Table 1.1, page 15-1.

Table 1.1 Coriant mTera Craft Station User's Guide Revision History

Revision	Change History	Release Date
A	Initial release for mTera UTP FP1.0.x.	6/14

Online Help

1.04 Content differences may exist between the online Help provided with this software and the corresponding *Craft Station User's Guide*. The most current information is published in the *Craft Station User's Guide*.

2. Installing the Craft Station

2.1 This section describes how to install the Craft Station software. You may install the software on a laptop running Windows® 2000, Windows® XP, or Windows® Vista Enterprise. Multiple sessions of the Craft Station can be running simultaneously in order to access multiple NEs. This section describes the following:

- Installing the Craft Station software onto the laptop. Contact your Coriant representative to confirm the part number of the most current CD. Refer to Installing the Craft Station Software on a PC or Laptop, page 15-3.
- Logging in to and out of the Craft Station. Refer to Logging In to the Craft Station, page 15-7, and Logging Out of the Craft Station, page 15-10.

Note: *In specific topologies, the Craft Station can run in configurations other than those that connect directly to an NE. The Craft Station can connect to NEs via a local area network (LAN) and to multiple NEs via an internal network provided on the GCC management channel.*

System Requirements

2.2 The Craft Station software runs on a Windows-based PC or laptop. Table 2.1, page 15-3 provides recommended minimum hardware and operating system requirements for PCs supporting the Craft Station.

Table 2.1 PC or Laptop Hardware and Operating System Requirements

PC Parameter	Required
Software	Microsoft Windows XP Professional with SP3, Microsoft Windows Vista Enterprise, or Microsoft Windows 7 with SP1
Additional Software	Java J2SE Runtime Environment 7.0 Update 21 or newer
Processor	Pentium III
RAM	1 GB
Hard Drive	20 GB
Optical Drive (only needed when installed via CD)	CD-ROM
Ethernet	10/100 Base T Fast Ethernet PCI Adapter
Serial Port	RS-232 or equivalent USB/RS-232 adapter
Video Card	8 MB PCI-bus, 1024 x 768 x 256 colors

Installing the Craft Station Software on a PC or Laptop

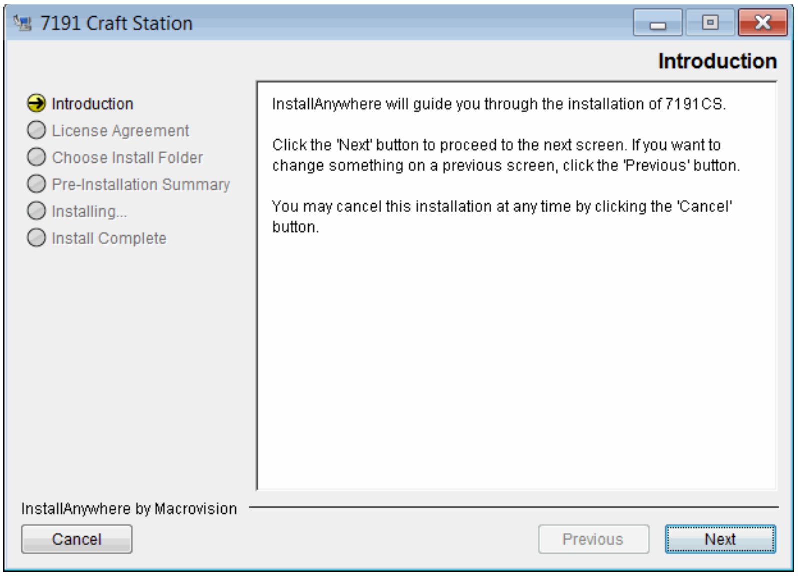
2.3 Install the Craft Station software onto the hard drive of a laptop or PC by performing the following steps:

Note: *Remove previous versions of the Craft Station before installing a new one. Refer to Uninstalling the Craft Station, page 15-10.*

__ 1. Insert the current Craft Station software CD into the CD drive of the computer. The opening screen of the Craft Station displays briefly, identifying the software.

__ 2. The **Introduction** dialog box of the software installer (InstallAnywhere®) launches automatically. Refer to Figure 2.1, page 15-4.

Figure 2.1 Installation Introduction



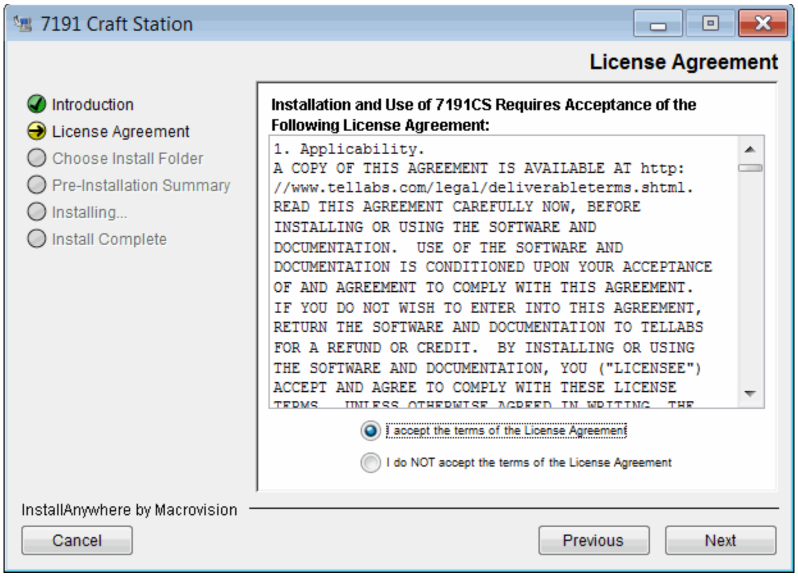
InstallAnywhere will guide you through the installation of 7191CS.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

__ 3. Read the text, then click **Next**. Refer to Figure 2.2, page 15-4.

Figure 2.2 Craft Station License Agreement



Installation and Use of 7191CS Requires Acceptance of the Following License Agreement:

```
1. Applicability.
A COPY OF THIS AGREEMENT IS AVAILABLE AT http:
//www.tellabs.com/legal/deliverableterms.shtml.
READ THIS AGREEMENT CAREFULLY NOW, BEFORE
INSTALLING OR USING THE SOFTWARE AND
DOCUMENTATION.  USE OF THE SOFTWARE AND
DOCUMENTATION IS CONDITIONED UPON YOUR ACCEPTANCE
OF AND AGREEMENT TO COMPLY WITH THIS AGREEMENT.
IF YOU DO NOT WISH TO ENTER INTO THIS AGREEMENT,
RETURN THE SOFTWARE AND DOCUMENTATION TO TELLABS
FOR A REFUND OR CREDIT.  BY INSTALLING OR USING
THE SOFTWARE AND DOCUMENTATION, YOU ("LICENSEE")
ACCEPT AND AGREE TO COMPLY WITH THESE LICENSE
TERMS.  UNLESS OTHERWISE AGREED IN WRITING, THE
```

● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

__ 4. Carefully read the license agreement.

__ Click the **I accept the terms of the License Agreement** button, and then click **Next** to accept the terms of the agreement and continue the installation.

__ Click the **I do NOT accept the terms of the License Agreement** button, and the **License Agreement Warning** box displays. Click **Quit** to end the installation. Or click **Resume** to return to the **License Agreement** dialog box.

__ 5. The **Choose Install Folder** dialog box displays. Refer to Figure 2.3, page 15-5.

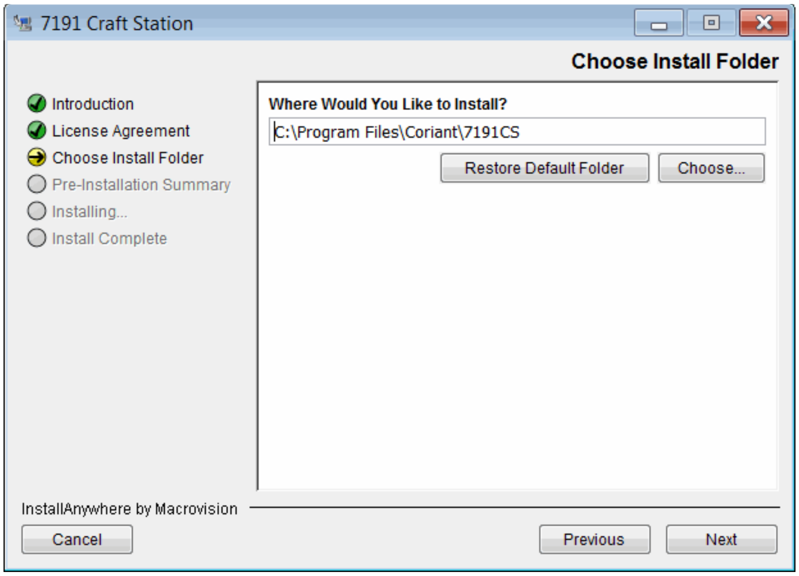
The Craft Station software defaults to the following installation directory: **C:\Program Files\Coriant\7191CS**.

__ Click **Choose** to change the installation directory.

__ To return to the default path, click **Restore Default Folder**.

__ Click **Next** to continue.

Figure 2.3 Choose Install Folder

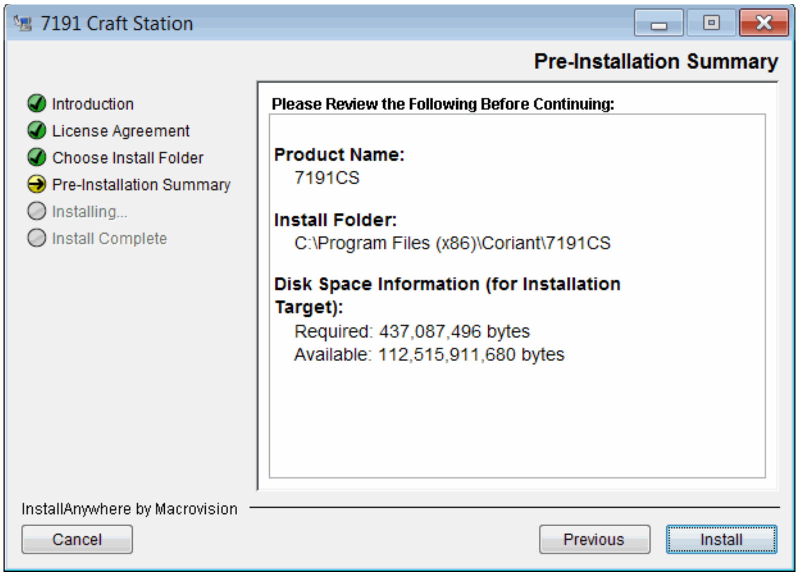


Where Would You Like to Install?

C:\Program Files\Coriant\7191CS

__ 6. The **Pre-Installation Summary** dialog box displays. Refer to Figure 2.4, page 15-6. Review the installation information displayed to confirm it is correct and then click **Install**. The installation program copies the software from the CD to the specified installation directory. A status bar displays at the bottom of the screen indicating the progress of the installation.

Figure 2.4 Pre-Installation Summary



Please Review the Following Before Continuing:

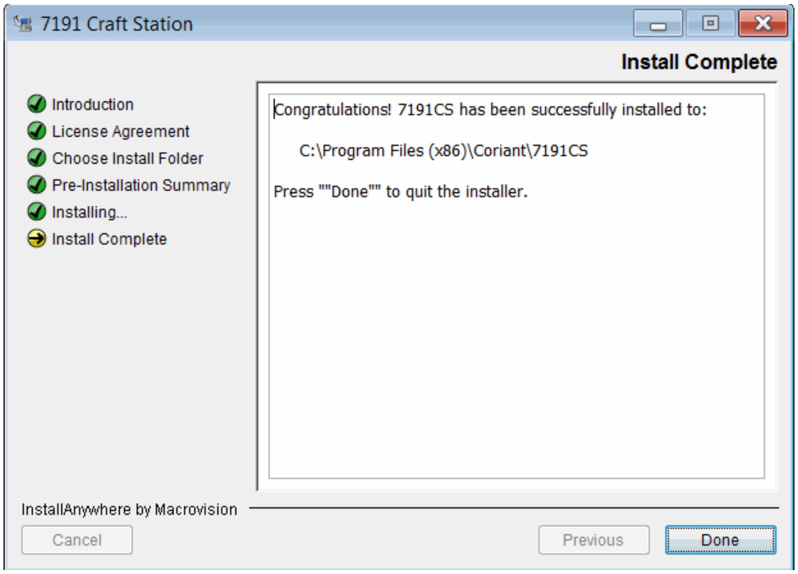
Product Name:
7191CS

Install Folder:
C:\Program Files (x86)\Coriant\7191CS

Disk Space Information (for Installation Target):
Required: 437,087,496 bytes
Available: 112,515,911,680 bytes

__ 7. When the installation completes, the **Install Complete** dialog box displays, confirming the success of the installation. Click **Done** to exit the installer program. Refer to Figure 2.5, page 15-6.

Figure 2.5 Install Complete



Congratulations! 7191CS has been successfully installed to:

C:\Program Files (x86)\Coriant\7191CS

Press ""Done"" to quit the installer.

__ 8. The installation program places a shortcut icon on the desktop. Double-click the icon to start the Craft Station.

Setting Up Notice and Consent Banner (Optional)

2.4 If your company's IT policy requires a notice and consent banner prior to login of the Craft Station, create and enable the Notice and Consent Banner by performing the following steps:

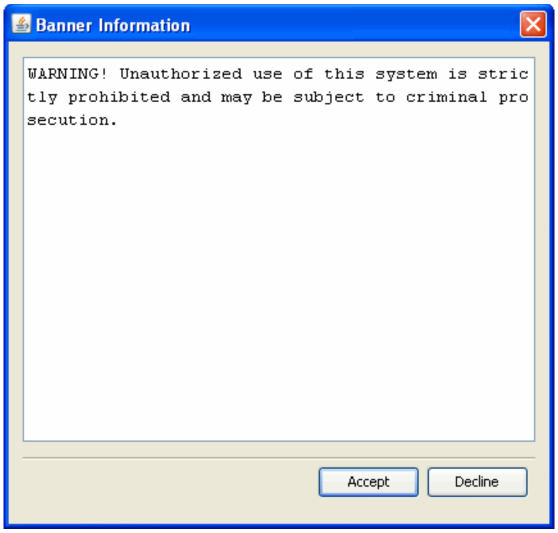
Note: *For information about how to edit the warning message that displays before connecting to an NE, refer to Editing NE Security Message, page 15-128. Or refer to the ED-WARNING command in TL1 Command Reference Manual. Click the Help menu in the Craft Station to access this document.*

__ 1. Create a text file with the notice and consent information. Name the file banner.txt.

__ 2. Copy the banner.txt file into the [CRAFT_INSTALL]\cfg directory.

__ 3. With the banner.txt file in the [CRAFT_INSTALL]\cfg directory, the Notice and Consent Banner displays prior to logging into the Craft Station. Refer to the example in Figure 2.6, page 15-7.

Figure 2.6 Notice and Consent Banner



```
WARNING! Unauthorized use of this system is stric
tly prohibited and may be subject to criminal pro
secution.
```

Logging In to the Craft Station

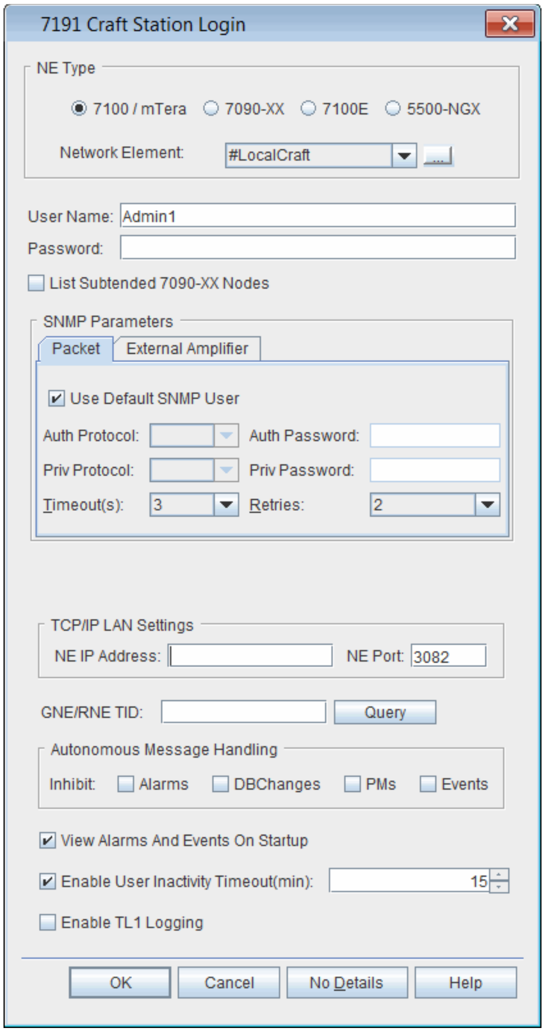
2.5 Before using the Craft Station to communicate with the NE, configure laptop IP settings and establish the LAN connection to the NE. Refer to Commissioning an NE, page 15-11.

2.6 Log in to and start the Craft Station by performing the following steps:

Note: *Log in to the Craft Station with NE administrator privileges for full functionality.*

__ 1. Double-click the **CS** shortcut icon on the desktop to start the Craft Station. The **Craft Station Login** dialog box displays. Refer to Figure 2.7, page 15-8.

Figure 2.7 Craft Station Login



7191 Craft Station Login

NE Type

● 7100 / mTera ○ 7090-XX ○ 7100E ○ 5500-NGX

Network Element: #LocalCraft

User Name: Admin1

Password:

□ List Subtended 7090-XX Nodes

SNMP Parameters

☑ Use Default SNMP User

Auth Protocol: Auth Password:

Priv Protocol: Priv Password:

Timeout(s): 3 Retries: 2

TCP/IP LAN Settings

NE IP Address: NE Port: 3082

GNE/RNE TID:

Autonomous Message Handling

Inhibit: □ Alarms □ DBChanges □ PMs □ Events

☑ View Alarms And Events On Startup

☑ Enable User Inactivity Timeout(min): 15

□ Enable TL1 Logging

__ 2. In the **NE Type** area, verify that **7100 / mTera** is selected.

__ 3. Type the **User name** and the **Password** in the respective boxes.

__ 4. Configure how the Craft Station handles autonomous messages using the **Autonomous Message Handling** area. Click **Alarms**, **DBChanges**, **PMs**, or **Events** to stop the Craft Station from receiving the respective autonomous messages from the NE. If you do not click the boxes, the Craft Station receives the respective autonomous messages from the NE.

- Click **Alarms** to stop the Craft Station from receiving REPT^ALM and REPT^ALM^ENV messages.
- Click **DBChanges** to stop the Craft Station from receiving REPT^DBCHG messages.
- Click **PMs** to stop the Craft Station to from receiving REPT^PM messages.
- Click **Events** to stop the Craft Station from receiving the following messages: REPT^BKUP, REPT^EVT, REPT^EVT^FXFR, REPT^RMV, REPT^RST, and REPT^EVT^SESSION.

__ 5. The user inactivity timeout option allows you to select the number of minutes after which the Craft Station disconnects the user if there is no activity. To disable this feature, un-check the **Enable User Inactivity Timeout** check box. To enable this feature, perform the following substeps:

__ 5.1 Click the **Enable User Inactivity Timeout** check box.

__ 5.2 Click the up and down arrows to set the number of minutes after which the Craft Station disconnects the user if there is no activity.

__ 6. The TL1 logging option allows you to save TL1 messages into a log file during a user session. The log filename consists of the NE TID, date, and time when the session was initiated. To enable this feature, click the **Enable TL1 Logging** check box. To disable this feature, un-check the **Enable TL1 Logging** check box.

__ 7. You can connect to an NE in several ways. Choose one of the following options:

Connecting to NE Through LCI Port

If you are connecting to the NE though the local craft port, refer to Installing the Craft Station, page 15-2 to verify that you have properly configured the laptop IP address and mask. Verify the NE IP Address box displays 10.0.0.1. (If you changed the NE IP Address from its default of 10.0.0.1, type the correct NE IP address.) Click **OK** to log into the NE. The main window of the Craft Station displays.

Session Timeout

2.7 For security purposes, the NE software supports a session timeout feature that is provisioned per TL1 user. If no user activity occurs for fifteen minutes, the NE TL1 user session times out, and the TL1 user must log in again. You may increase or decrease this value at the **Modify TL1 User** dialog box. By default, the Enable User Inactivity Timeout parameter is enabled in the Craft Station. To cancel the timeout function, click to un-check the **Enable User Inactivity Timeout** check box in the **Login** dialog box. Refer to Figure 2.7, page 15-8.

Exiting the Craft Station

2.8 This section describes how to exit the Craft Station.

Logging Out of the Craft Station

2.9 Log out of the Craft Station by performing the following steps:

__ 1. Click **File**.

__ 2. Click **Logout**.

__ 3. Click **OK** in the **Confirmation** box. The Craft Station closes your session and the **Login** dialog box displays.

Closing the Craft Station

2.10 Exit the Craft Station by performing the following steps:

__ 1. Click **File**.

__ 2. Click **Exit**.

__ 3. Click **OK** in the **Confirmation** box.

Uninstalling the Craft Station

2.11 Uninstall the Craft Station software by performing the following steps:

__ 1. On the Windows Desktop, click the **Start** button, and select **Control Panel**.

__ 2. Double-click the **Add or Remove Programs** item. The **Add or Remove Programs** dialog box displays.

__ 3. Scroll through the list to the Craft Station icon labeled **CS**.

__ 4. Click **Change/Remove**.

__ 5. When the **Uninstall CS** dialog box displays, click **Cancel** or **Uninstall**.

3. Commissioning an NE

3.1 This section describes how to use the Craft Station to simplify NE turn-up using the basic commissioning tool.

Backward Compatibility

3.2 You can use the FP11.0.x Craft Station to connect to NEs supporting FP1.0.x.

Note: *If you attempt to connect to an NE that is beyond the supported compatibility range, the Craft Station generates a warning message after login.*

Basic Commissioning

3.3 The basic commissioning tool allows quick turn-up of individual NEs. Before beginning, confirm that the site meets the following pre-requisites:

__ The Craft Station software is installed on the laptop.

__ The STPM is the only module seated in the shelf in slot **25**.

__ The SDM is seated in the shelf in slot **33**.

__ Current NE software is accessible on a CD or PC/laptop hard drive.

__ The laptop is set with a default IP address of:

10.0.0.2

with a subnet mask of:

255.255.255.0

__ An Ethernet-to-LCI port connection exists between the laptop and the STPM.

__ An Ethernet connection exists between the laptop and the SDM debug port. This connection can be from a second Ethernet adapter bridged on the laptop or an external hub.

__ NE configuration and IP specifications are available.

Basic Commissioning Procedure

3.4 This section explains how to commission a single NE. The prerequisites listed in paragraph 3.03, page 15-11 must be in place.

Setting Up FTP

3.05 The Craft Station must start an FTP server so that software can upload files to the NE. If an FTP server is already running on the PC when the Craft Station attempts to start its FTP server, a dialog box displays allowing the current FTP server to be shut down or to configure the Craft Station FTP server for a different port.

3.6 Set up the FTP server to a different port by performing the following steps:

__ 1. On the laptop, navigate to the Craft Station software files folder. For example:

c:\Coriant\ProgramFiles\7191CS\

__ 2. Expand the folder named **7191CS** until you see the subdirectory named **cfg**.

__ 3. In the **cfg** folder, open the file named **emsSettings** using Wordpad.

__ 4. Scroll through the file and modify the following lines so they read as described here:

__ `TLAB_FTPHOMEDIR`=\\<home directory for FTP files>

__ `TLAB_FTPSERVERPORT=2000` (or other unused TCP port on the PC)

__ 5. From the **File** menu, click **Save**.

__ 6. Exit the **emsSettings** file.

Setting Up the Network Interface

3.7 The following procedures connect a computer that is equipped with a Microsoft Windows based operating system and is used to transfer the application software to the STPM and SDM. Perform the following procedures to connect the portable computer to the STPM and SDM to install the application software and to set up the network interface parameters.

Note: *Depending on your Windows operating system, the path to get to the Network Connection may be different than what is described here.*

Warning:

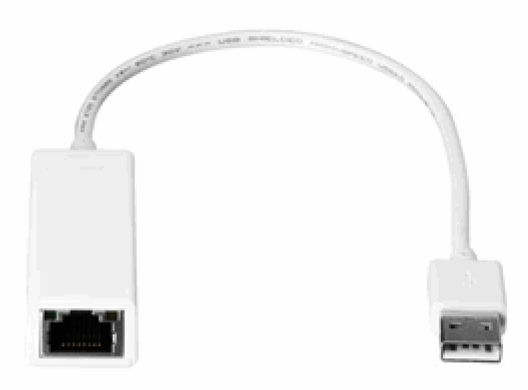
Electrostatic discharge (ESD) may damage sensitive electronic components resulting in a traffic-affecting condition. Ensure that plug-in modules are stored in static preventive material. Do not touch any components on the modules. Handle modules by the edges or front panel. Always wear a properly grounded wrist strap when handling, removing, or inserting a module and when touching the equipment shelves or cables. ESD protective flooring, used with proper ESD footwear, may be used as an alternative to a wrist strap. ESD wrist straps and footwear should be checked daily to verify performance.

__ 1. Attach an antistatic wrist strap to your wrist and connect it to the wrist strap jack, located on the front of a heat baffle. Alternately, use an ESD foot strap and ESD protective flooring. Be sure the ESD protective flooring is kept clean to ensure a good discharge path.

__ 2. Log in to the portable computer with the Windows-based operating system.

Note: *To basic commission an mTera system, two Ethernet connections are required. This is accomplished via a hub or by installing a second Ethernet adapter via USB. Refer to Figure 3.1, page 15-13 for an example of an Ethernet-to-USB adapter.*

Figure 3.1 Ethernet Adapter



__ 3. Bridge the Ethernet adapters together (this allows one IP address to be used for both connections) by performing the following substeps:

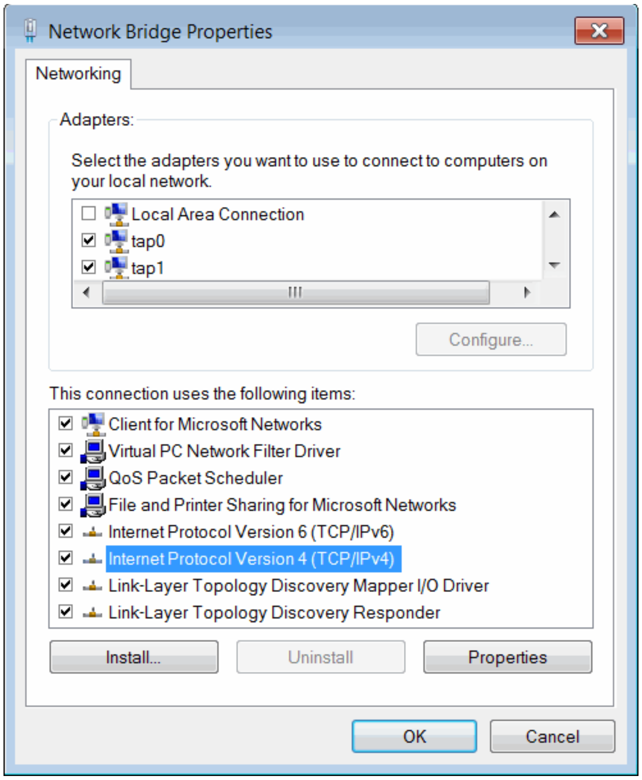
__ 3.1 On the PC, navigate to **Control Panel** and select **Network Connections**.

__ 3.2 Using the **Ctrl** key, highlight both Ethernet adapters.

__ 3.3 Right-click one of the highlighted Ethernet adapters and select **Bridge Connections**. A Network Bridge icon displays.

__ 3.4 Right-click the **Network Bridge** icon to view the shortcut menu, then click **Properties**. The **Network Bridge Properties** dialog box displays. Refer to Figure 3.2, page 15-14.

Figure 3.2 Network Bridge Properties



Network Bridge Properties

Networking

Adapters:

Select the adapters you want to use to connect to computers on your local network.

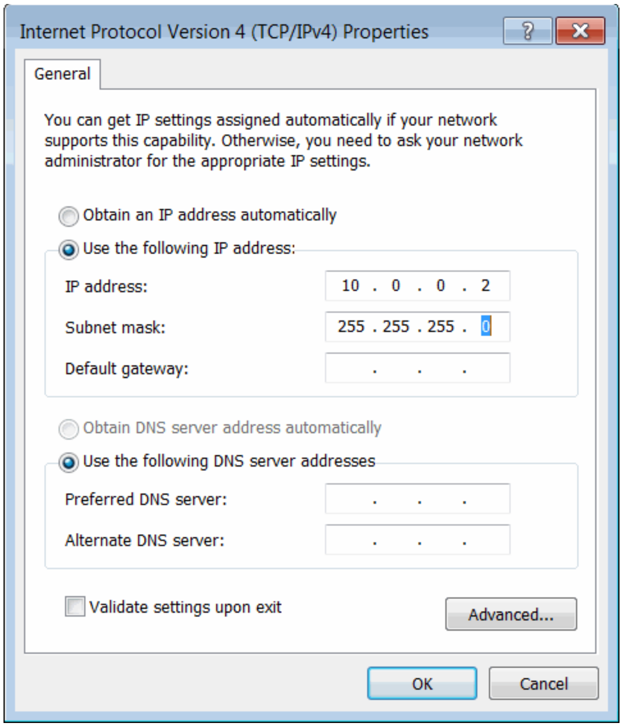
☐ Local Area Connection
☑ tap0
☑ tap1

This connection uses the following items:

☑ Client for Microsoft Networks
☑ Virtual PC Network Filter Driver
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

__ 4. Click to highlight **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box displays. Refer to Figure 3.3, page 15-14.

Figure 3.3 Internet Protocol Version 4 Properties



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 10 . 0 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses

Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit

__ 4.1 Verify the **Use the following IP address:** radio button is selected. Type the following values in the **IP address:** and **Subnet mask:** fields, respectively.

IP address: **10.0.0.2**

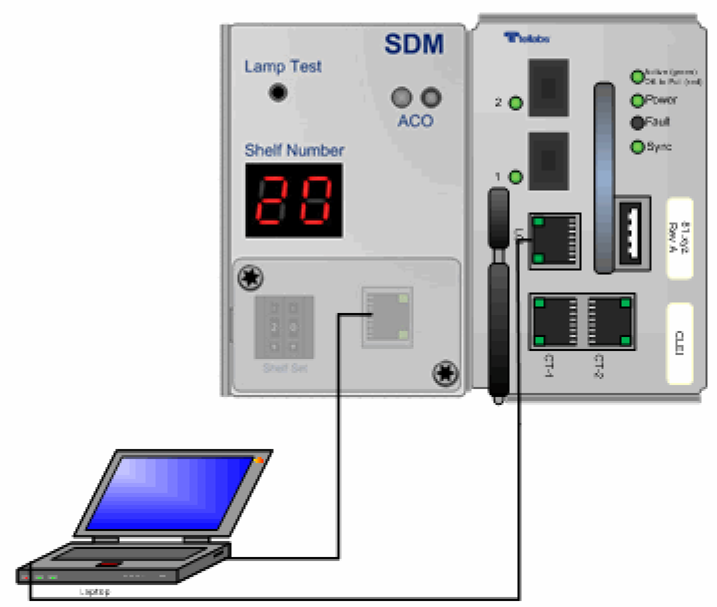
Subnet mask: **255.255.255.0**

__ 5. Verify the **Shelf Number** and **Shelf Num Sel** on the **SDM** are set to **20**.

__ 6. From the computer, connect an Ethernet cable between the computer and the **Debug** connector on the mTera shelf SDM. Refer to Figure 3.4, page 15-15.

__ 7. From the same computer, connect an Ethernet cable between the computer and the **LCI** (Local Craft Interface) port on the STPM in slot 25. Refer to Figure 3.4, page 15-15.

Figure 3.4 Cable Connections on the SDM and STPM



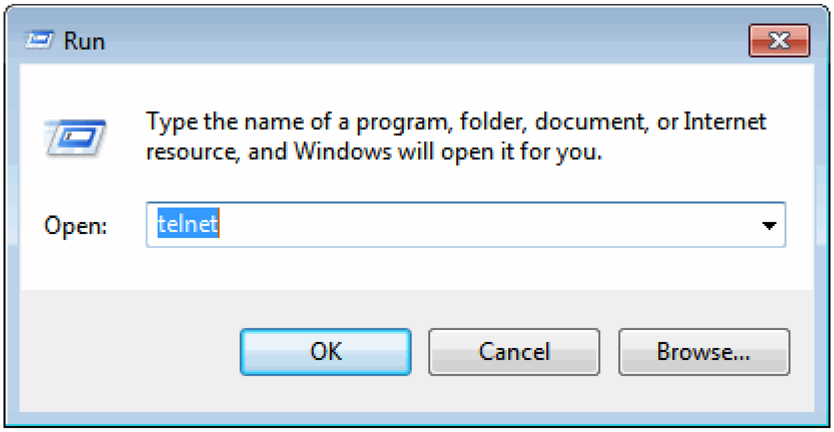
Go to Setting Up the User Interface, page 15-15.

Setting Up the User Interface

3.8 Set up the user interface to the system by completing the following steps:

__ 1. On the Windows based computer, click the **Start** button in the lower left corner of the desk top. From the Start menu, click **Programs**. From the Programs submenu, click **Accessories** and then click **Run**. The run window displays. Refer to Figure 3.5, page 15-16.

Figure 3.5 Run



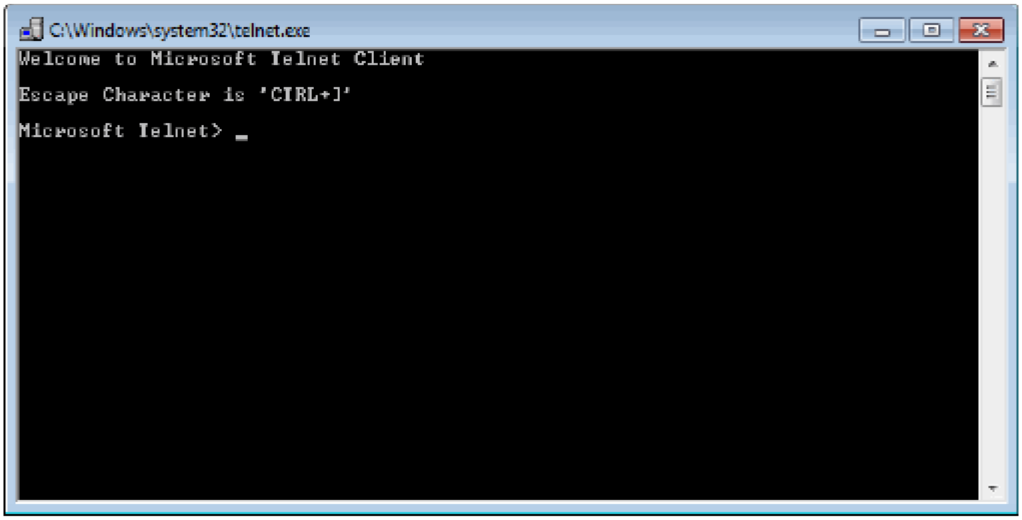
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet

__ 2. In the **Open** field, type **telnet**.

__ 3. Click **OK**. A **telnet** window opens. Refer to Figure 3.6, page 15-16.

Figure 3.6 Telnet



```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> _
```

__ 4. In the **Telnet** window, type **o** (for open) and then press **Enter**.

System response:
`< to >`

__ 5. Type **10.0.0.5 7125** and press **Enter**. This opens a serial connection to the SPTM in slot 25.

System response:
`Connecting to 10.0.0.5 ...`

__ 6. Reseat the STPM in slot 25.

__ 7. Wait for the system to display the following prompt.

```
## TLAB: OS recovery invoked ...

Initiating download/save of /mnt/sdcard/ACTIVE/STPMos.tlf.  Attempt #1

** Trying to retrieve /mnt/sdcard/ACTIVE/STPMos.tlf through SD...

***********************************************

SD_Client: Sending load request
```

__ 8. Type **QQ** in the Telnet window. The system resets.

System response:

```
POST memory PASSED

Flash: 128 MiB

L2:    128 KB enabled

Corenet Platform Cache: 2048 KB enabled

MMC:  FSL_SDHC: 0

PCIe1: Root Complex, no link, regs @ 0xfe200000

PCIe1: Bus 00 - 00

In:    serial

Out:   serial

Err:   serial

Net:   Initializing Fman

Fman1: Uploading microcode version 101.8.0

Fman2: Uploading microcode version 101.8.0

FM1@TGEC1, FM2@TGEC1

Type "uboot" to stop autoboot:

=>
```

__ 9. When prompted, type **uboot** to stop autoboot and press **Enter**.

Note: *It is a very short window where the uboot prompt is displayed, and it is possible to miss the prompt. If you miss the prompt, return to step 7, page 15-17.*

Loading Software from a CD-ROM

3.9 Load the software to the mTera shelf from a CD-ROM by performing the following steps. This procedure takes 15 minutes.

__ 1. Copy FP9_0_ZZ321_20140316_MTERA.zip and FP9_0_ZZ321_20140316_MTERA.dcr files to the directory. The directory name should not include a blank.

__ 2. Install the Craft Station software. Refer to Installing the Craft Station Software on a PC or Laptop, page 15-3.

__ 3. Change STPM console password to be null by following operation.

```
telnet SDM_IP 7100 (ex. telnet 172.29.160.113 7100)

Connected to 172.29.160.113:7100 configuration server

SDM 172.29.160.113>pwd Admin

Please input password:

Please input password again:

Admin Password changed success
```

__ 4. Open Windows Explorer and navigate to the **7191CS** folder.

__ 5. Expand the folder named **7191CS** until you see the subdirectory named **cfg**.

__ 6. In the **cfg** folder, open the file named **emsSettings** using Wordpad.

__ 7. Scroll to section labeled `TLAB_BASICCOMMISSION`. Modify the `TLAB_BASICCOMMISSION` line to read:

TLAB_BASICCOMMISSION=true

__ 8. Scroll to section labeled `TLAB_BC_USE_DCN`. Modify the `TLAB_BC_USE_DCN` line to read:

TLAB_BC_USE_DCN=true

Note: *This setting determines if CS allows user to FTP by DCN port when BC.*

__ 9. Scroll to section labeled `TLAB_BC_MAX_SESSION_NUM`. Modify the `TLAB_BC_MAX_SESSION_NUM` line to read:

TLAB_BASICCOMMISSION=true

__ 10. Scroll to section labeled `TLAB_BC_MAX_SESSION_NUM`. Modify the `TLAB_BC_MAX_SESSION_NUM` line to read:

#TLAB_BC_MAX_SESSION_NUM=100

Note: *Set the max session number for the user Admin1. Remove the "#" to set the number.*

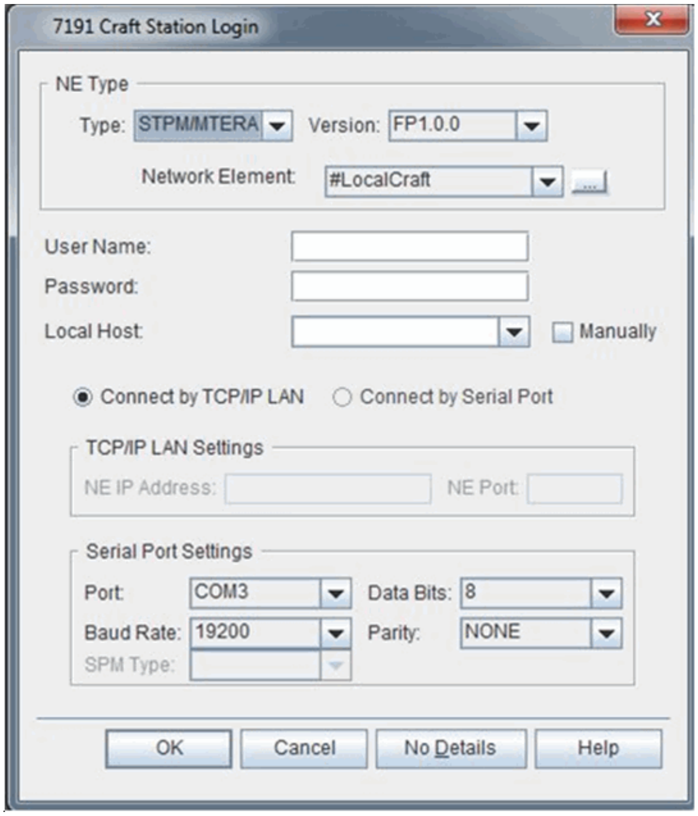
__ 11. From the **File** menu, click **Save**.

__ 12. Exit the **emsSettings** file.

__ 13. Double-click the **Craft Station** icon on the desktop. A confirmation box displays asking if you want to basic commission the NE.

__ 14. Click **OK**. The **Craft Station Login** dialog box displays. Refer to Figure 3.7, page 15-19.

Figure 3.7 Basic Commissioning Initial Login



7191 Craft Station Login

NE Type

Type: STPM/MTERA Version: FP1.0.0

Network Element: #LocalCraft

User Name:

Password:

Local Host: □ Manually

● Connect by TCP/IP LAN ○ Connect by Serial Port

TCP/IP LAN Settings

NE IP Address: NE Port:

Serial Port Settings

Port: COM3 Data Bits: 8

Baud Rate: 19200 Parity: NONE

SPM Type:

__ 15. At the **Login** window, type your default user name and password.

Note: *If you do not have the default user name and password, contact Coriant Technical Assistance Center at http://www.coriant.com/services_support for assistance.*

__ 16. Select **STPM/MTERA** from the **Type** drop-down menu.

__ 17. Select **FP1.0** from the **Version** drop-down menu.

__ 18. Click the button labeled **Connect by Serial Port**. The **Serial Port Settings** box is activated.

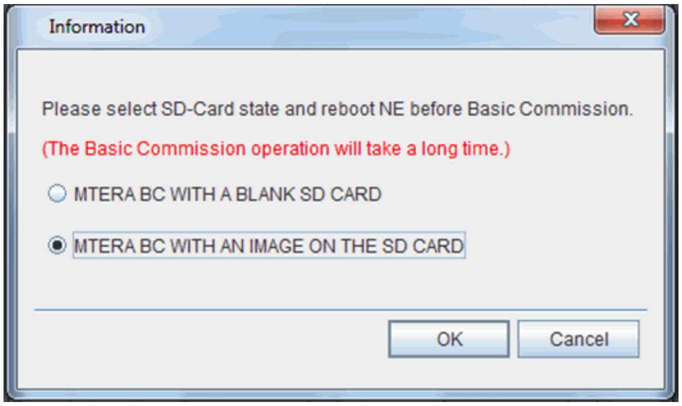
__ 19. Verify the following values are selected in the **Serial Port Settings** box:

Port = COM1
Data Bits = 8
Baud Rate = 19200 (automatically selected)
Parity = None

Note: *The communications port selected is typically COM Port 1. Select the COM Port that corresponds to the RS-232 port interfacing the NE.*

__ 20. Click **OK**. An Information box displays. Refer to Figure 3.8, page 15-20.

Figure 3.8 Information



Information

Please select SD-Card state and reboot NE before Basic Commission.

(The Basic Commission operation will take a long time.)

○ MTERA BC WITH A BLANK SD CARD

● MTERA BC WITH AN IMAGE ON THE SD CARD

__ 21. Choose one of the following options:

- If you are performing basic commissioning using an STPM that is new from the factory (and therefore has a blank SD card), choose **MTERA BC WITH A BLANK SD CARD**.
- If you are performing basic commissioning using an existing STPM that contains an image on its SD card, choose **MTERA BC WITH AN IMAGE ON THE SD CARD**.

__ 22. In a telnet window, type **10.0.0.5 7125** and press **Enter**. This opens a serial connection to the SPTM in slot 25.

System response:

```
Connecting to 10.0.0.5 ...
```

__ 23. Depending on the current state of the STPM, enter the command to reboot the STPM:

- If current state is FC, reboot NE by following command:

```
STPM:FC:20.25> shutdown cold
```

- If current state is SMA, reboot NE by following command:

```
root@stpm_20_25:~# reboot
```

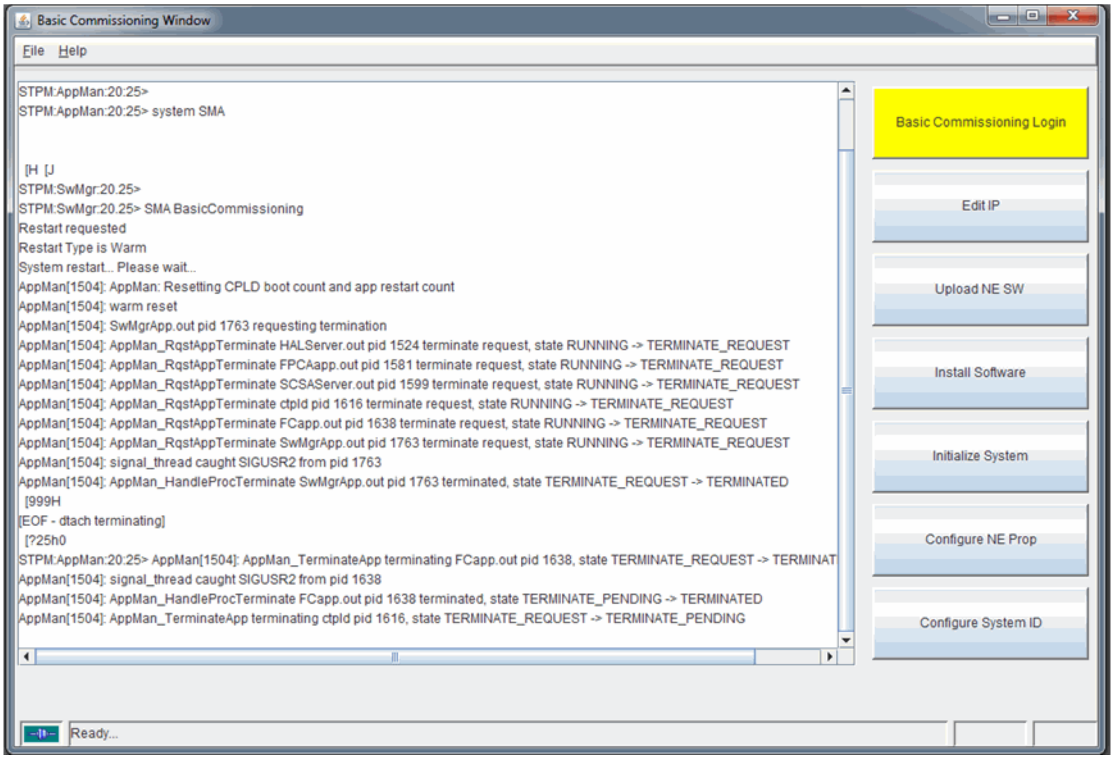
- If current state is STPM, reboot NE by following command:

```
STPM:AppMan:20:25> shutdown cold
```

__ 24. When reboot finishes (less then five minutes), close or quit telnet GUI because of only one session for STPM.

__ 25. After the STPM reboots, click **OK** in the Information box (in Figure 3.8, page 15-20) to start basic commissioning. The **Basic Commissioning Window** displays. Refer to Figure 3.9, page 15-21.

Figure 3.9 Basic Commissioning Window



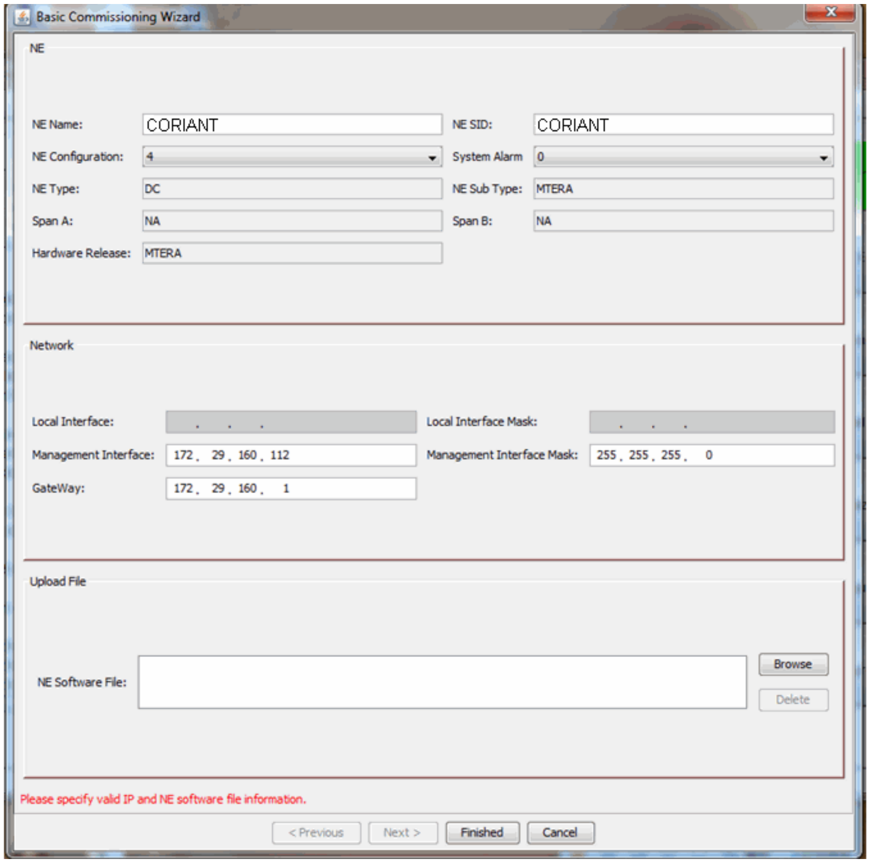
```
STPM:AppMan:20:25>
STPM:AppMan:20:25> system SMA


 [H [J
STPM:SwMgr:20.25>
STPM:SwMgr:20.25> SMA BasicCommissioning
Restart requested
Restart Type is Warm
System restart... Please wait...
AppMan[1504]: AppMan: Resetting CPLD boot count and app restart count
AppMan[1504]: warm reset
AppMan[1504]: SwMgrApp.out pid 1763 requesting termination
AppMan[1504]: AppMan_RqstAppTerminate HALServer.out pid 1524 terminate request, state RUNNING -> TERMINATE_REQUEST
AppMan[1504]: AppMan_RqstAppTerminate FPCAapp.out pid 1581 terminate request, state RUNNING -> TERMINATE_REQUEST
AppMan[1504]: AppMan_RqstAppTerminate SCSAServer.out pid 1599 terminate request, state RUNNING -> TERMINATE_REQUEST
AppMan[1504]: AppMan_RqstAppTerminate ctpld pid 1616 terminate request, state RUNNING -> TERMINATE_REQUEST
AppMan[1504]: AppMan_RqstAppTerminate FCapp.out pid 1638 terminate request, state RUNNING -> TERMINATE_REQUEST
AppMan[1504]: AppMan_RqstAppTerminate SwMgrApp.out pid 1763 terminate request, state RUNNING -> TERMINATE_REQUEST
AppMan[1504]: signal_thread caught SIGUSR2 from pid 1763
AppMan[1504]: AppMan_HandleProcTerminate SwMgrApp.out pid 1763 terminated, state TERMINATE_REQUEST -> TERMINATED
 [999H
[EOF - dtach terminating]
 [?25h0
STPM:AppMan:20:25> AppMan[1504]: AppMan_TerminateApp terminating FCapp.out pid 1638, state TERMINATE_REQUEST -> TERMINAT
AppMan[1504]: signal_thread caught SIGUSR2 from pid 1638
AppMan[1504]: AppMan_HandleProcTerminate FCapp.out pid 1638 terminated, state TERMINATE_PENDING -> TERMINATED
AppMan[1504]: AppMan_TerminateApp terminating ctpld pid 1616, state TERMINATE_REQUEST -> TERMINATE_PENDING
```

Ready...

__ 26. Set NE properties and network. Refer to Figure 3.10, page 15-21

Figure 3.10 Basic Commissioning Wizard



NE Name: CORIANT
NE SID: CORIANT
NE Configuration: 4
System Alarm: 0
NE Type: DC
NE Sub Type: MTERA
Span A: NA
Span B: NA
Hardware Release: MTERA

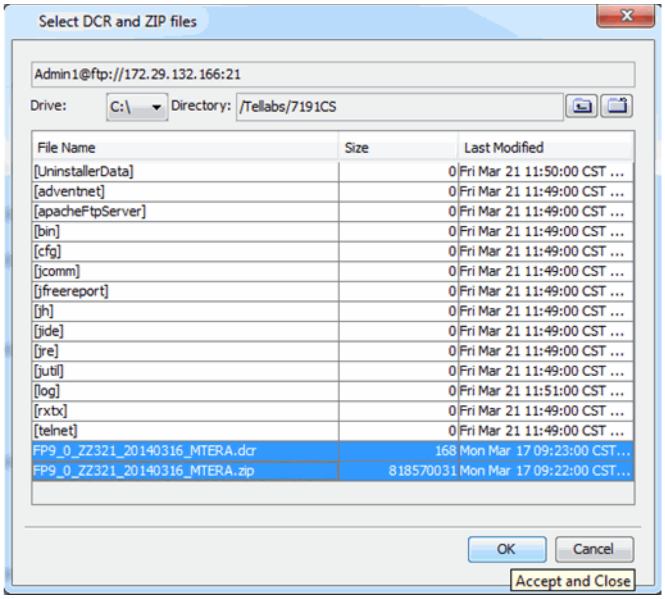
Local Interface: . . .
Local Interface Mask: . . .
Management Interface: 172 . 29 . 160 . 112
Management Interface Mask: 255 . 255 . 255 . 0
GateWay: 172 . 29 . 160 . 1

NE Software File:

Please specify valid IP and NE software file information.

__ 27. In the Upload File area, click Browse button to select DCR and ZIP files. Use the **Ctrl** key to select both a **dcr** and a **zip** file. When you click the **Finished** button in this dialog box, the Craft Station provisions the NE with the parameters selected in the basic commissioning wizard. The Craft Station uploads, installs, and initializes the NE software. Confirm that the parameters selected to this point in the **Basic Commissioning Wizard** are correct and click **Finished**.

Figure 3.11 Select DCR and ZIP Files



Select DCR and ZIP files

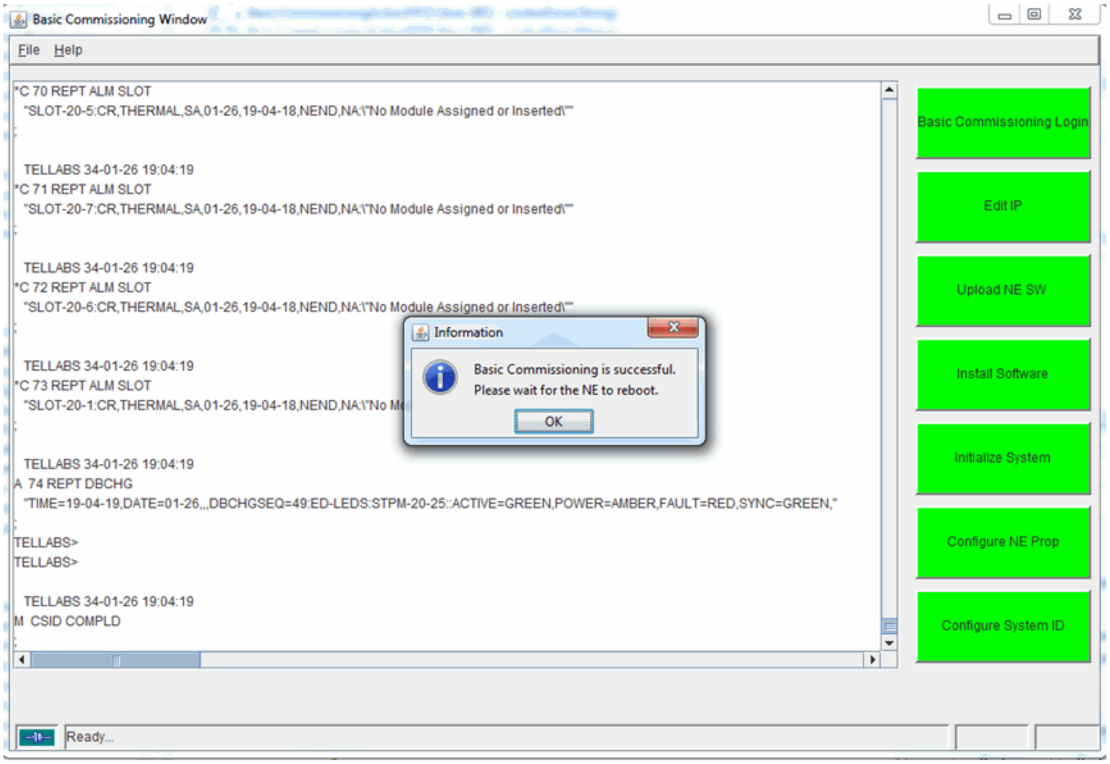
Admin1@ftp://172.29.132.166:21

Drive: C:\ Directory: /Tellabs/7191CS

File Name	Size	Last Modified
[UninstallerData]	0	Fri Mar 21 11:50:00 CST ...
[adventnet]	0	Fri Mar 21 11:49:00 CST ...
[apacheFtpServer]	0	Fri Mar 21 11:49:00 CST ...
[bin]	0	Fri Mar 21 11:49:00 CST ...
[cfg]	0	Fri Mar 21 11:49:00 CST ...
[jcomm]	0	Fri Mar 21 11:49:00 CST ...
[jfreereport]	0	Fri Mar 21 11:49:00 CST ...
[jh]	0	Fri Mar 21 11:49:00 CST ...
[jide]	0	Fri Mar 21 11:49:00 CST ...
[jre]	0	Fri Mar 21 11:49:00 CST ...
[jutil]	0	Fri Mar 21 11:49:00 CST ...
[log]	0	Fri Mar 21 11:51:00 CST ...
[rxtx]	0	Fri Mar 21 11:49:00 CST ...
[telnet]	0	Fri Mar 21 11:49:00 CST ...
FP9_0_ZZ321_20140316_MTERA.dcr	168	Mon Mar 17 09:23:00 CST...
FP9_0_ZZ321_20140316_MTERA.zip	818570031	Mon Mar 17 09:22:00 CST...

__ 28. Click **OK**. The Craft Station automatically runs basic commissioning, step by step. A status bar displays on the right side of the screen. Status buttons display in gray before basic commissioning executes. Status buttons display yellow when the action is in-progress and green when the action completes.

Figure 3.12 Basic Commissioning Window



```
*C 70 REPT ALM SLOT
  "SLOT-20-5:CR,THERMAL,SA,01-26,19-04-18,NEND,NA:\"No Module Assigned or Inserted\""
;

  TELLABS 34-01-26 19:04:19
*C 71 REPT ALM SLOT
  "SLOT-20-7:CR,THERMAL,SA,01-26,19-04-18,NEND,NA:\"No Module Assigned or Inserted\""
;

  TELLABS 34-01-26 19:04:19
*C 72 REPT ALM SLOT
  "SLOT-20-6:CR,THERMAL,SA,01-26,19-04-18,NEND,NA:\"No Module Assigned or Inserted\""
;

  TELLABS 34-01-26 19:04:19
*C 73 REPT ALM SLOT
  "SLOT-20-1:CR,THERMAL,SA,01-26,19-04-18,NEND,NA:\"No Mo
;

  TELLABS 34-01-26 19:04:19
A  74 REPT DBCHG
  "TIME=19-04-19,DATE=01-26,,,DBCHGSEQ=49:ED-LEDS:STPM-20-25::ACTIVE=GREEN,POWER=AMBER,FAULT=RED,SYNC=GREEN,"
;
TELLABS>
TELLABS>

  TELLABS 34-01-26 19:04:19
M  CSID COMPLD
;
```

Basic Commissioning is successful.
Please wait for the NE to reboot.

The Craft Station performs the following actions without any user intervention. Watch the status buttons on the right side of the screen to identify in-progress actions and completed actions.

__ When you click the **Finished** button in the previous screen, the **Upload NE Software** starts and the status button displays yellow. The NE software includes the **dcr** and **zip** files. A transfer progress bar tracks the activity.

__ When the Craft Station uploads the **dcr** and **zip** files to the NE, the **Upload NE Software** status button displays green. The software installation starts, and the **Install Software** status button displays yellow. An installation progress bar tracks the activity.

__ When software installation is complete, the **Install Software** status button displays green. The Craft Station send the initialize system command to the NE and the **Initialize System** status button displays yellow. The initialize system command causes a warm restart of the system processor module (STPM). After the processor module restarts, the software loads.

__ After the system reboots and the software loads, the **Configure NE Properties** action occurs. The Craft Station provisions the NE with the parameters entered in the **Basic Commissioning Wizard**. The **Configure NE Properties** status button displays yellow.

__ The system processor module (STPM) reboots. When the STPM restores, the **Configure NE Properties** status button displays green, and the **Configure System ID** status button displays yellow.

__ The Craft Station software captures the system name entered in the **Basic Commissioning Wizard** to configure the **System ID** and sends it to the NE.

__ When the Craft Station configures the System ID, the **Configure System ID** status button displays green and the **Configure Network** button displays yellow. The Craft Station provisions the NE with the EON and IP parameters entered into the basic commissioning wizard.

__ The system processor module (STPM) reboots. Before the STPM completes the reboot, the **Configure Network** status button displays green and an **Information** box displays. Click **OK**. All status buttons in the commissioning tool display green.

Note: *The STPM basic commissioning process can take up to 60 minutes. Wait until the Active LED on the STPM is a steady green, indicating commissioning is complete, before continuing. You cannot log in to the NE until after the NE completes the reboot.*

__ 29. From the **File** menu, click **Exit** to close the basic commissioning tool.

__ 30. Click **Yes** in the **Confirmation** box.

4. Navigating the Craft Station

4.1 This section describes how to navigate the screens, dialog boxes, and menus that comprise the Craft Station.

Craft Station Windows

4.2 The Craft Station is a graphical interface. The main window is comprised of three windows. Click and hold the border of any of the three windows to make the windows larger or smaller. The navigational aids provided in the Craft Station are typical Windows tools.

- Work in the **Navigation Window** to perform provisioning tasks.
- Right-click modules in the **Chassis View Window** to view module current states and modify settings.
- Access information on NE alarms and events in the **Notification Window**.

Navigation Window

4.3 The **Navigation Window** displays all of the autodiscovered system entities:

- network element
- Control Plane
- General Communications Channel
- Switch Domain (if present)
- shelves
- modules
- facilities
- cross-connects
- database (NE database management)
- software (NE software management)
- SNMP (TID mapping)
- telemetry (environmental alarms and external contacts)

4.4 Expand or collapse objects in this window depending on the view required. As each object expands, the Craft Station retrieves the elements below it. As this occurs, the display may delay for several seconds before it is refreshed. Expand modules to display the associated facilities, and expand facilities to show associated cross-connects.

4.5 The state of an object in the **Navigation Window** is either IS (In-Service) or OOS (Out-of-Service). Objects in the IS state display as black, and objects in the OOS state display as red. The state of an object changes in the object's **Properties** dialog box. Access the **Properties** dialog box by right-clicking the object.

Chassis Window

4.6 The **Chassis Window** provides a graphical representation of the shelves, modules, and ports that comprise the NE. In the **Chassis Window**, you can right-click any module and access all provisioning and maintenance actions associated with that module. The module LEDs show real-time status. You can also right-click any empty slot and access the **Create Module** dialog box. The **Create Module** dialog box shows only the modules allowed in the selected slot.

Notification Window

4.7 The **Notification Window** displays all of the current alarms and events set on the NE. Click the **Alarm** tab to view alarms. Click the **Event** tab to view events. Click the **TL1 Messages** tab to view all the TL1 messages and TL1 notifications sent and received by the Craft Station. Click the **SNMP Messages** tab to view SNMP communications with the packet subsystem. The **Alarm** and **Event** tabs display the following information: alarm severity, the related NE, entity type, detailed location of entity (AID), alarm severity, if the alarm is service affecting, the time and date the alarm/event was set, sequence when set, brief description of alarm, location and direction in network, and the relevant TL1 response. New alarms and events display as they are set. When a problem condition clears, alarms and events are automatically removed.

Alarm Tab

4.08 When you select the **Alarm** tab, use the buttons at the top of the **Notification Window** to manage the display. Click any field to change the alarm display to ascending or descending order, based on the field clicked. For example, click the **Set Time** field, and the alarms display newest to oldest.

4.9 Click the **Show Filters** button to define which alarms display and the number of alarms to display. Refer to Figure 4.1, page 15-28.

4.10 Click the **Filter Criteria** tab. Use the following alarm conditions as filters:

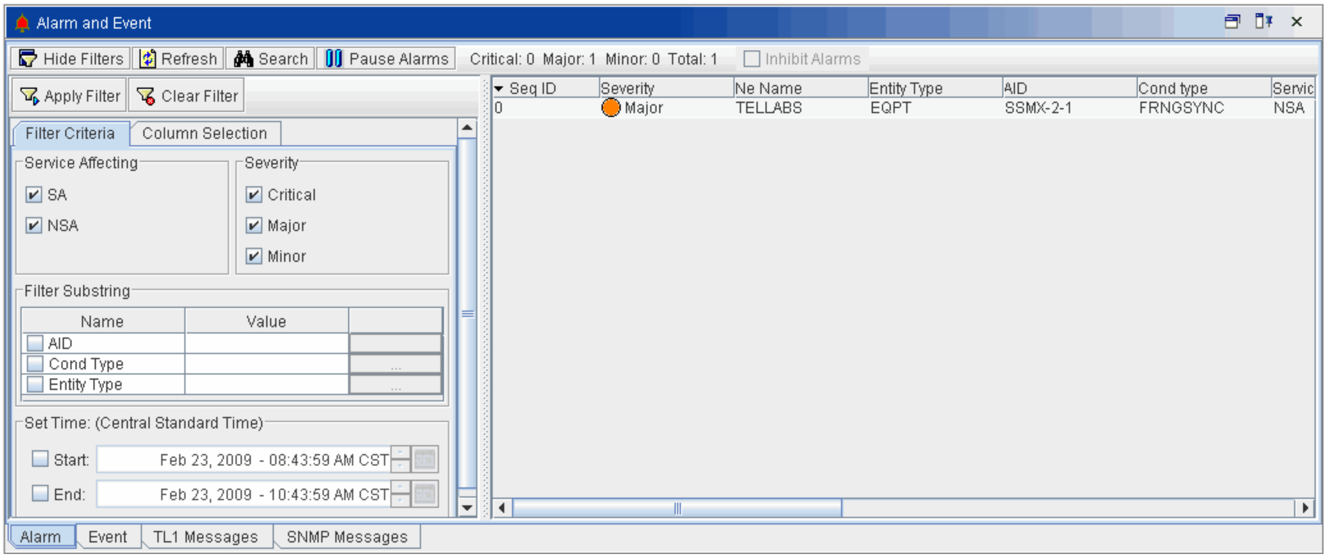
- **Service Affecting**: Click **SA** (service affecting), or **NSA** (non-service affecting) to select the service-affecting nature of the alarms you want captured and displayed. Critical alarms are automatically defined as service-affecting.
- **Severity**: Click **Critical**, **Major**, or **Minor** to select the severity of alarms to capture and display.
- **Filter Substring**: Click the **AID**, **Cond Type**, or **Entity Type** box to filter alarms by a substring. Type the substring value in the **Value** column.
- **Set Time**: Click the **Start** and **End** boxes to filter alarms according to a time period. Use the up and down arrows to change the start and end time values.
- Click **Apply Filter** to make the selections active.
- Click **Clear Filter** to reset the filters.
- Click **Hide Filters** to close the **Show Filters** dialog box.

4.11 Click the **Column Selection** tab. In the **Visible** column, click the check boxes to display the following column names in the alarm table:

- Seq ID
- Severity
- Ne Name
- Entity Type
- AID
- Cond type
- Service Affecting
- NE Set Time
- Location
- Direction
- Description
- TL1 Response

Or, in the **Set Visible** box, click **All** to enable the Craft Station to display all column names. Click **None** to disable all of the column name selections.

Figure 4.1 Alarm Window - Show Filters



Critical: 0 Major: 1 Minor: 0 Total: 1

Service Affecting

☑ SA

☑ NSA

Severity

☑ Critical

☑ Major

☑ Minor

Filter Substring

Name	Value
□ AID	
□ Cond Type	
□ Entity Type	

Set Time: (Central Standard Time)

□ Start: Feb 23, 2009 - 08:43:59 AM CST

□ End: Feb 23, 2009 - 10:43:59 AM CST

Seq ID	Severity	Ne Name	Entity Type	AID	Cond type	Servic
0	● Major	TELLABS	EQPT	SSMX-2-1	FRNGSYNC	NSA

4.12 Click **Refresh** to retrieve all current alarms.

4.13 Click **Search** to search the list of alarms using specified text. Type key words into the **Find Text** box of the **Find Text** dialog box. The Craft Station saves previous search entries; access these entries by clicking the drop-down box.

Note: *Entries in the* ***Find Text*** *box are case-sensitive.*

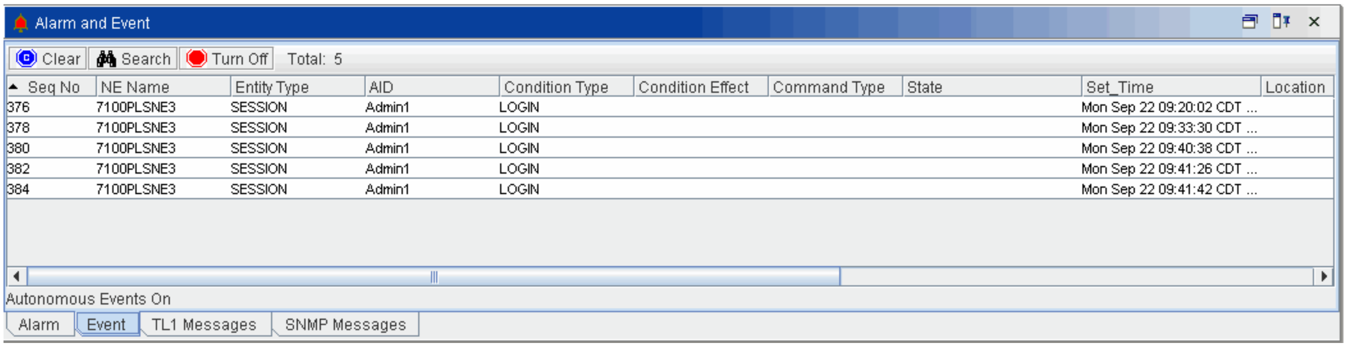
4.14 Click the **Pause Alarms** button to stop reporting new alarms. Click it again (displays as **Continue Alarms**) to resume alarm reporting.

4.15 The **Total** field at the top of the **Alarm Window** reports the total number of alarms currently displayed.

Event Tab

4.16 Click the **Event** tab in the **Notification Window** to display events set against the NE. New events display as they are set. Clear events by clicking the blue octagon icon in the **Event Window**. Refer to Figure 4.2, page 15-28.

Figure 4.2 Main Window - Event Tab



Total: 5

Seq No	NE Name	Entity Type	AID	Condition Type	Condition Effect	Command Type	State	Set_Time	Location
376	7100PLSNE3	SESSION	Admin1	LOGIN				Mon Sep 22 09:20:02 CDT ...	
378	7100PLSNE3	SESSION	Admin1	LOGIN				Mon Sep 22 09:33:30 CDT ...	
380	7100PLSNE3	SESSION	Admin1	LOGIN				Mon Sep 22 09:40:38 CDT ...	
382	7100PLSNE3	SESSION	Admin1	LOGIN				Mon Sep 22 09:41:26 CDT ...	
384	7100PLSNE3	SESSION	Admin1	LOGIN				Mon Sep 22 09:41:42 CDT ...	

Autonomous Events On

4.17 Use the following icons at the top of the **Event Window** to manage the events displayed:

- Click the **Blue Octagon** icon to clear all displayed events.
- Click the **Binocular** icon to search the list of events using specified text.

Note: *Entries in the **Text to find** box are case-sensitive.*

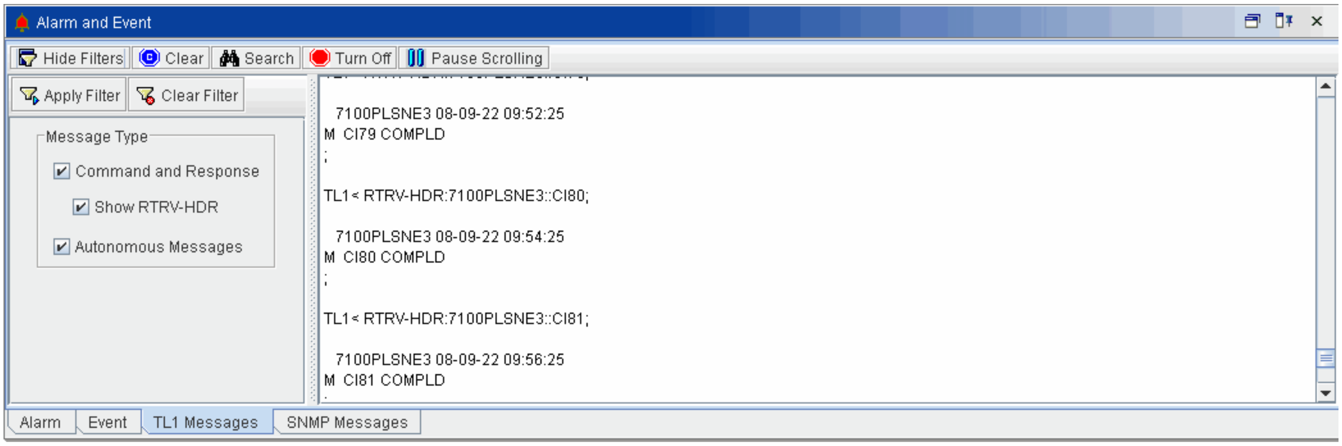
- Click the **Red Octagon** icon to stop reporting new events. Click it again (it displays as a **Green Octagon**) to resume event reporting.
- The **Total** field at the top of the screen reports the total number of alarms currently displayed.

TL1 Message Tab

4.18 Click the **TL1 Message** tab in the **Notification Window** to display all the TL1 messages/notifications the Craft Station sends and receives.

4.19 Click **Show Filters** to define which TL1 messages should display. Refer to Figure 4.3, page 15-29.

Figure 4.3 TL1 Messages - Show Filters



Message Type

☑ Command and Response

☑ Show RTRV-HDR

☑ Autonomous Messages

```
  7100PLSNE3 08-09-22 09:52:25
M  CI79 COMPLD
;

TL1< RTRV-HDR:7100PLSNE3::CI80;

  7100PLSNE3 08-09-22 09:54:25
M  CI80 COMPLD
;

TL1< RTRV-HDR:7100PLSNE3::CI81;

  7100PLSNE3 08-09-22 09:56:25
M  CI81 COMPLD
```

4.20 You can select the following TL1 message types as filters:

- Click **Command and Response** to show TL1 commands and system responses.
- Click **Show RTRV-HDR** to show heartbeat commands and system responses between the Craft Station and the NE.
- Click **Autonomous Message** to show TL1 autonomous messages that are automatically generated by the system.
- Click **Apply Filter** to make the selections active.
- Click **Clear Filter** to reset the filters.
- Click **Hide Filters** to close the **Show Filters** dialog box.

4.21 Click **Clear** to clear the TL1 message box.

4.22 Click **Search** to search the list of TL1 messages using specified key words. Type key words into the **Find Text** box of the **Find Text** dialog box. The Craft Station saves previous search entries; these can be accessed by clicking the drop-down box.

Note: *Entries in the **Find Text** box are case-sensitive.*

4.23 Click **Turn On** to allow new TL1 messages to scroll in the box. Click it again (displays as **Turn Off**) to stop new TL1 messages from displaying in the box.

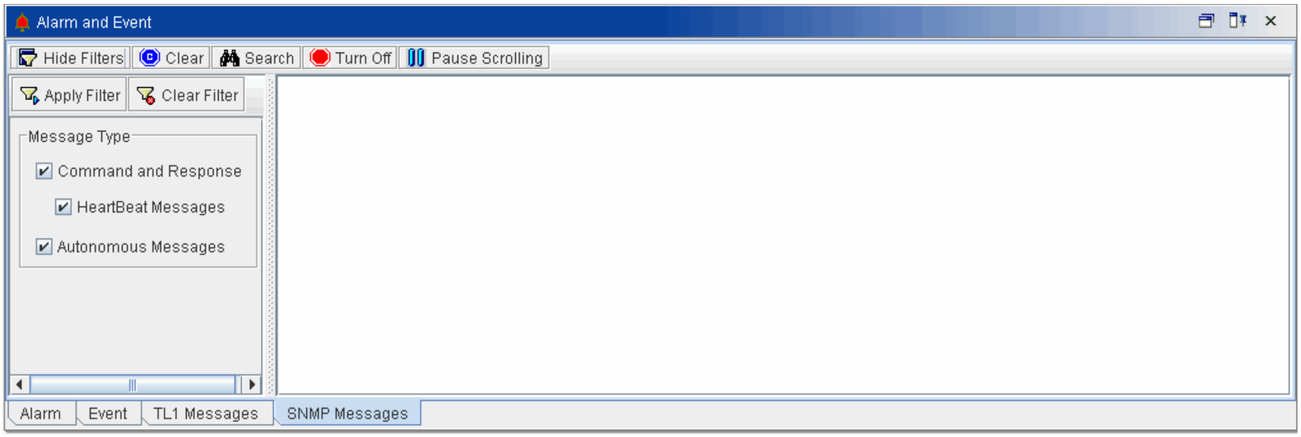
4.24 Click **Pause Scrolling** to stop new TL1 messages from scrolling in the box. This feature is useful if you want to pause the TL1 output to focus on a particular message. Click it again (displays as **Continue Scrolling**) to allow TL1 messages to continue scrolling in the box.

SNMP Messages Tab

4.25 Click the **SNMP Messages** tab in the **Notification Window** to display SNMP messages sent to an NE that contains a packet subsystem. New SNMP messages display as they are sent. Clear SNMP messages by clicking the blue octagon icon in the **Alarm and Event** window. Refer to Figure 4.4, page 15-30.

Note: *For more information about using the Craft Station to manage the packet subsystem, refer to Packet Subsystem Operations Management Systems (EMS and CS).*

Figure 4.4 Main Window - SNMP Messages Tab



☑ Command and Response

☑ HeartBeat Messages

☑ Autonomous Messages

4.26 You can select the following SNMP message types as filters:

- Click **Command and Response** to show commands and system responses.
- Click **Heartbeat Messages** to show keep-alive messages sent between the Craft Station and the NE.
- Click **Autonomous Message** to show autonomous messages that are automatically generated by the system.
- Click **Apply Filter** to make the selections active.
- Click **Clear Filter** to reset the filters.
- Click **Hide Filters** to close the **Show Filters** dialog box.

4.27 Use the following icons at the top of the **Alarm and Event Window** to manage the events displayed:

- Click the **Blue Octagon** icon to clear all displayed events.
- Click the **Binocular** icon to search the list of events using specified text.
- Click the **Red Octagon** icon to stop reporting new events. Click it again (it displays as a **Green Octagon**) to resume event reporting.

Navigating the Menus

4.28 The main menus of the Craft Station interface provide selections to access most of the tasks required for provisioning system elements.

File Menu

4.29 The **File** menu provides access to logging in to and out of the NE, and exiting the Craft Station.

View Menu

4.30 The **View** menu manages the active state and the display of the three main windows.

Fault Menu

4.31 The **Fault** menu launches dialog boxes manage performance monitoring, facility, equipment, and logical alarm profile tables.

Security Menu

4.32 The **Security** menu provides access to TL1 user management, TL1 session management, and IP security management.

Actions Menu

4.33 The **Actions** menu launches dialog boxes to manage the NE and the objects below it. The menu selections vary based on the object selected in the **Navigation Window**. You can also right-click an object in the **Navigation Window** to access the tasks provided in the **Actions** menu.

Reports Menu

4.34 The **Reports** menu provides to the equipment, facility, and entity reports supported by the Craft Station.

Tools Menu

4.35 The **Tools** menu provides access to the **External AMP Setup** wizard. Refer to *7100 OTS OLA Acceptance Testing, 7100 OTS SBOADM Acceptance Testing*, *7100 Nano SBOADM Acceptance Testing*, and *7100 Nano OLA Acceptance Testing* for more information about installing a 71125A Network Interfaced Raman (NIR), 71125B Co-Propagating Raman Amplifier 700 mW (CRA), or 71128A Booster Amplifier (BAMP).

4.36 The **Tools** menu also provides access to the **External AMP Craft**. Use the External AMP Craft to manage the NIR, CRA, or BAMP.

Help Menu

4.37 The **Help** menu provides system information about the Craft Station and access to technical documentation.

Craft Station Autodiscovery

4.38 The autodiscovery feature of the Craft Station reports the NE hardware configuration at system startup and each time a user expands or modifies an element in the **Navigation Window**. The NE continually surveys itself to identify new hardware elements and then reports this information to the Craft Station.

4.39 The NE displays a management information tree (MIT) in the **Navigation Window** and graphically in the **Chassis Window**. In the **Navigation Window**, you can expand or collapse views of the NE elements. When icons display as red, they are out-of-service. When the icons display as black, they are in-service. In the **Chassis Window**, visual aids include real-time LED activity and module faceplates that display yellow when in-service and gray when out-of-service. The module acronym on the faceplate displays red when the module is out-of-service. The module acronym displays black when the module is in-service.

Note: *Right-click the parent of any object to view the shortcut menu, then click* ***Refresh*** *to start autodiscovery.*

5. User and Session Management

5.1 The Craft Station provides menu selections that allow an Administrative level user to manage users and sessions. This section describes how to implement these features.

Note: *Refer to TL1 Command Reference Manual for additional details on TL1 user and session settings. Click the Help menu in the Craft Station to access this document.*

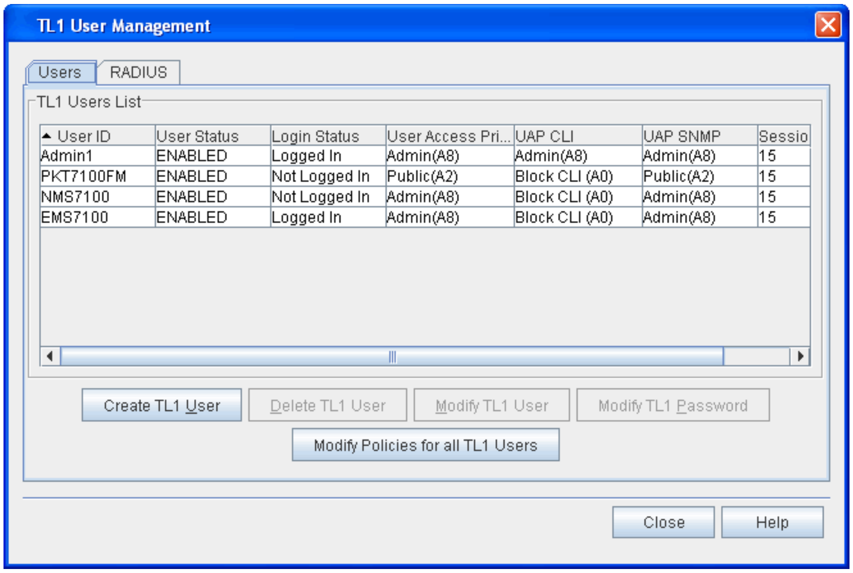
TL1 User Management

5.2 Use the Craft Station to access and manage TL1 user accounts. A Craft Station user with A8 (Admin privileges) can add, delete, modify, and reset passwords for TL1 user accounts. The following procedures describe how to implement these actions:

- Creating a TL1 User, page 15-34
- Setting TL1 User Account Policy, page 15-38
- Deleting a TL1 User, page 15-40
- Modifying a TL1 User Profile, page 15-41
- Changing a TL1 User Password, page 15-44
- Retrieving TL1 Logs, page 15-47
- Retrieving AO Logs, page 15-48

5.3 To provision user access, right-click the NE icon in the **Navigation Window** to view the shortcut menu, then click **TL1 User Management**. The **TL1 User Management** dialog box displays. Refer to Figure 5.1, page 15-33.

Figure 5.1 TL1 User Management



▲ User ID	User Status	Login Status	User Access Pri...	UAP CLI	UAP SNMP	Sessio
Admin1	ENABLED	Logged In	Admin(A8)	Admin(A8)	Admin(A8)	15
PKT7100FM	ENABLED	Not Logged In	Public(A2)	Block CLI (A0)	Public(A2)	15
NMS7100	ENABLED	Not Logged In	Admin(A8)	Block CLI (A0)	Admin(A8)	15
EMS7100	ENABLED	Logged In	Admin(A8)	Block CLI (A0)	Admin(A8)	15

5.4 The **TL1 User Management** dialog box provides the following information about current TL1 Users:

- User ID
- User Status
- Login Status
- User Access Privilege
- UAP CLI
- UAP SNMP
- Session Time Out (min)

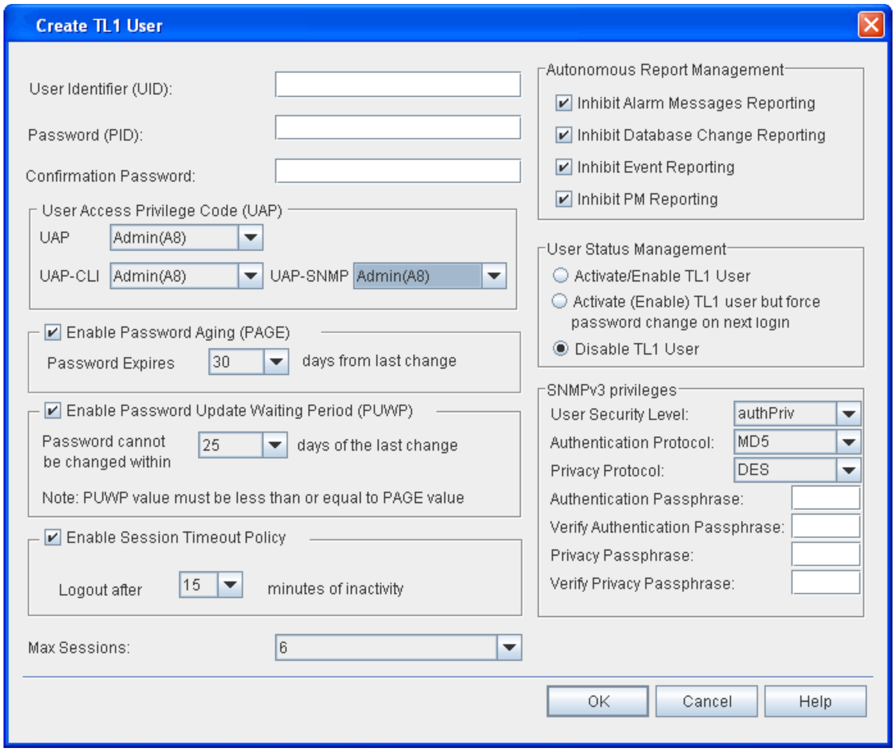
Creating a TL1 User

5.5 Create a TL1 user by performing the following steps:

Note: *To modify the account of a TL1 user, refer to Modifying a TL1 User Profile, page 15-41.*

__ 1. In the **TL1 User Management** dialog box, click **Create TL1 User**. Refer to Figure 5.1, page 15-33. The **Create TL1 User** dialog box displays. Refer to Figure 5.2, page 15-34.

Figure 5.2 Create TL1 User



Create TL1 User

User Identifier (UID):

Password (PID):

Confirmation Password:

User Access Privilege Code (UAP)

UAP: Admin(A8)

UAP-CLI: Admin(A8) UAP-SNMP: Admin(A8)

☑ Enable Password Aging (PAGE)

Password Expires 30 days from last change

☑ Enable Password Update Waiting Period (PUWP)

Password cannot be changed within 25 days of the last change

Note: PUWP value must be less than or equal to PAGE value

☑ Enable Session Timeout Policy

Logout after 15 minutes of inactivity

Max Sessions: 6

Autonomous Report Management

☑ Inhibit Alarm Messages Reporting

☑ Inhibit Database Change Reporting

☑ Inhibit Event Reporting

☑ Inhibit PM Reporting

User Status Management

○ Activate/Enable TL1 User

○ Activate (Enable) TL1 user but force password change on next login

● Disable TL1 User

SNMPv3 privileges

User Security Level: authPriv

Authentication Protocol: MD5

Privacy Protocol: DES

Authentication Passphrase:

Verify Authentication Passphrase:

Privacy Passphrase:

Verify Privacy Passphrase:

__ 2. Type the user ID in the **User Identification (UID)** box (6–20 alphanumeric characters).

__ 3. Type a password in the **Password (PID)** box.

Note: *The password must conform to the password complexity requirements set for the NE. Refer to System Administration Using TL1 or System Administration Using Management Systems for password requirements.*

__ 4. Type the password again in the **Confirm Password** box.

__ 5. The User Access Privilege Code (UAP) area contains drop-down boxes to set the UAP for system privileges, CLI privileges, and SNMP privileges.

In the **UAP** drop-down box, select the access privilege code for the user.

The user access privilege code (UAP) represents the functional group and authorization level assigned to each Craft Station user. The UAP indicates what actions the user can execute. The UAPs and associated system privileges are:

- Administrator or Admin (A8)
- Operator (A7)
- Provisioning (A6)
- Test (A4)
- Public (A2)
- Block CLI (A0)

A8 is the highest user level, and A2 is the lowest. The A8 user can perform all Craft Station actions. The A7 user can administer all TL1 commands excluding security commands, user account administration, and digital certificate administration. The A6 user can perform all Craft Station actions except for setting system and user security and administering user accounts. The A4 user can provision, cancel, and release system elements. The A2 user can edit his or her own password, cancel actions, and view dialog boxes. The A0 user cannot use the CLI cut-through feature to control packet operations or access the SNMP interface. All users can receive autonomous messages as defined by the system administrator.

In the **UAP-CLI** drop-down box, select the access privilege code for the user.

The user access privilege code-command line interface (UAP-CLI) represents the functional group and authorization level assigned each Craft Station user for the CLI cut-through. The UAP-CLI indicates what actions the user can execute. The UAP-CLIs and associated system privileges are:

- Operator (A7)
- Provisioning (A6)
- Test (A4)
- Public (A2)
- Block CLI (A0)

A7 is the highest user level, and A2 is the lowest. The A7 user can administer all CLI commands excluding security commands, user account administration, and digital certificate administration. The A6 user can perform all CLI actions except for setting system and user security and administering user accounts. The A4 user can provision, cancel, and release system elements. The A2 user can edit command their own password, cancel actions, and retrieve information. The A0 user cannot use the CLI cut-through feature to control packet operations or access the SNMP interface. All users can receive autonomous messages as defined by the system administrator.

In the **UAP-SNMP** drop-down box, select the access privilege code for the user.

The user access privilege code-simple network management protocol (UAP-SNMP) represents the functional group and authorization level assigned each Craft Station user for SNMP. The UAP-SNMP indicates what actions the user can execute. The UAP-SNMPs and associated system privileges are:

Administrative (A8)

Public (A2)

Block SNMP (A0)

The A8 user has full read and write access to all SNMP MIBs.The A2 user has full read-only and notify access to the MIBs, and write access to change the user's own SNMP passphrase. The A0 user is blocked from accessing the SNMP interface.

__ 6. Select or deselect the box beside **Enable Password Aging (PAGE)**. If you select the box, click the number of days until the password expires from the **Password Expires** drop-down box. The system begins the count from the day the user modified his or her password. This field supports any value between **1** and **255** days.

__ 7. Select or deselect the box beside **Enable Password Update Waiting Period (PUWP)** and select the number of days before the password can be changed. This field defines the number of days that a user must wait before changing their password. This field supports any value between **1** and **60** days.

Note: *The PUWP value must be less than or equal to the value selected in the PAGE field (step 6, page 15-36).*

__ 8. Select or deselect the box beside **Enable Session Timeout Policy to enable system timeout**. This field defines the number of minutes the system waits before it times-out based on a period when no system activity is initiated by the user. This field supports any value between **1** and **99** minutes.

__ 9. In the **Autonomous Report Management** box, select the messages that you do not want displayed for this user profile. Click any of the check boxes below to suppress the type of message described:

__ **Inhibit Alarm Messages Reporting**: Click this check box to inhibit messages displayed when an alarm condition on the system sets or clears.

__ **Inhibit Database Change Reporting**: Click this check box to inhibit messages displayed when provisioned system settings change or a user performs an external action is to the system, such as inserting a module.

__ **Inhibit Event Reporting**: Click this check box to inhibit messages displayed when a system event occurs. Events include a change in status condition or a system irregularity that is not severe enough to prompt an alarm.

__ **Inhibit PM Reporting**: Click this check box to inhibit messages displayed when user-provisioned performance monitoring parameters report.

__ 10. In the **User Status Management** box, select the status you want to assign this user. Status values are:

__ **Activate/Enable TL1 User**: The user has access to the system when provisioning in this dialog box is complete, and you click the **OK** button.

__ **Activate (Enable) TL1 user but force password change on next login**: The user has access to the system when provisioning in this dialog box is complete, and you click the **OK** button. But, the user must change his or her password the first time they log in.

__ **Disable TL1 User**: The user will not have access to the system.

__ 11. If you set the UAP SNMP privilege to A2 or A8 in step 5, page 15-35, the SNMPv3 privileges area becomes active. Select the SNMPv3 protocol options by performing the following steps. Otherwise, go to step 12, page 15-38.

__ 11.1 Click the **User Security Level** drop-down box to select **authPriv** (authorization and privacy), **authNoPriv** (authorization but no privacy), or **noAuthnoPriv** (no authorization and no privacy).

__ 11.2 Click the **Authentication Protocol** drop down box to select **MD5** or **SHA**.

__ 11.3 Select the **Privacy Protocol** drop down box to select **DES**.

__ 11.4 Type the authentication passphrase in the **Authentication Passphrase** box. This parameter is mandatory if the user security level is authPriv.

__ 11.5 Type the authentication passphrase in the **Verify Authentication Passphrase** box.

__ 11.6 Type the privacy passphrase in the **Privacy Passphrase** box. This parameter is mandatory if the user security level is authPriv.

__ 11.7 Type the privacy passphrase in the **Verify Privacy Passphrase** box.

__ 12. Click the **Max Sessions** drop-down box to select the maximum number of sessions allows for a user (**1**–**128**, default is **6**).

__ 13. Click **OK** to apply changes. Click **Cancel** to close this dialog box without applying the changes.

Setting TL1 User Account Policy

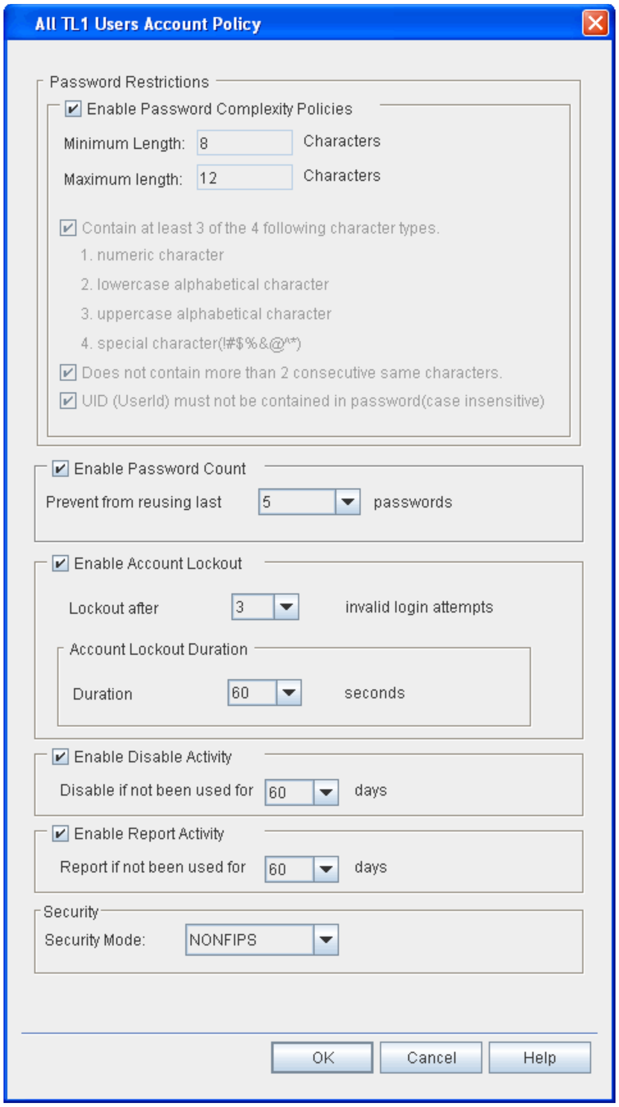
5.6 A user with Administrator (A8) privileges can define the parameters within which passwords can be defined. Define these parameters in the **All TL1 Users Account Policy** dialog box. Define the parameters by performing the following steps:

__ 1. From the **Actions** menu, click **TL1 User Management**. The **TL1 User Management** dialog box displays. Refer to Figure 5.1, page 15-33.

__ 2. In the **TL1 User Management** dialog box, click the **Modify Policies for all TL1 Users** button.

__ 3. The **All TL1 Users Account Policy** dialog box displays. Refer to Figure 5.3, page 15-39.

Figure 5.3 TL1 Users Account Policy



All TL1 Users Account Policy

Password Restrictions

☑ Enable Password Complexity Policies

Minimum Length: 8 Characters

Maximum length: 12 Characters

☑ Contain at least 3 of the 4 following character types.

1. numeric character
2. lowercase alphabetical character
3. uppercase alphabetical character
4. special character(!#$%&@^*)

☑ Does not contain more than 2 consecutive same characters.

☑ UID (UserId) must not be contained in password(case insensitive)

☑ Enable Password Count

Prevent from reusing last 5 passwords

☑ Enable Account Lockout

Lockout after 3 invalid login attempts

Account Lockout Duration

Duration 60 seconds

☑ Enable Disable Activity

Disable if not been used for 60 days

☑ Enable Report Activity

Report if not been used for 60 days

Security

Security Mode: NONFIPS

__ 4. In the **Password Restrictions** box, select or deselect **Enable Password Complexity Policies**.

When you select this feature, login passwords must be between 8 and 12 characters in length, with at least three of the four following character types must be present: numeric character, lowercase alphabetical character, uppercase alphabetical character, and special character. Special characters consist of the following: ! # $ % & @ ^ *.

__ 5. Select or deselect **Enable Password Count**. This feature defines the number of previously used passwords (associated with this user) that cannot be reused. Select this value from the drop-down box.

__ 6. Select or deselect **Enable Account Lockout**. This feature defines the maximum number of consecutive and invalid login attempts before the Craft Station suspends the account.

__ 6.1 Click the **Lockout after** drop-down box to select the number of allowable **invalid login attempts** before the Craft Station locks the account.

__ 6.2 Click the **Duration** drop-down box to select the account lockout duration seconds. If the number of invalid login attempts exceeds the number defined, the Craft Station locks the account for a duration of **1** to **300** seconds.

__ 7. Select or deselect **Enable Disable Activity**. This feature allows the system administrator to specify the number of days after which the NE disables an unused account.

__ 7.1 Click the **Disable if not been used for** drop-down box to select the number of days (**1**–**365**) for the inactivity threshold.

__ 8. Select or deselect **Enable Report Activity**. This feature allows the system administrator to specify the number of days after which the NE issues an autonomous message regarding an unused account.

__ 8.1 Click the **Report if not been used for** to select the number of days (**1**–**365**) for the inactivity report threshold.

Note: *The values specified in the Enable Disable Activity box and Enable Report Activity box do not apply to TL1 users with the A8 permission level.*

__ 9. Click the **Security Mode** drop-down box to specify whether system security is operating in FIPS compliance mode (**NONFIPS** or **FIPS**).

__ 10. Click **OK** to apply changes. An **Information** box displays confirming the changes have been made.

Deleting a TL1 User

5.7 To delete a TL1 user, click the **Actions** menu, and then click **TL1 User Management**. The **TL1 User Management** dialog box displays. Refer to Figure 5.1, page 15-33.

__ 1. Select the user to delete in the **TL1 Users List**.

__ 2. Click **Delete TL1 User**. A **Confirmation** box displays.

__ 3. Click **OK** or **Cancel**.

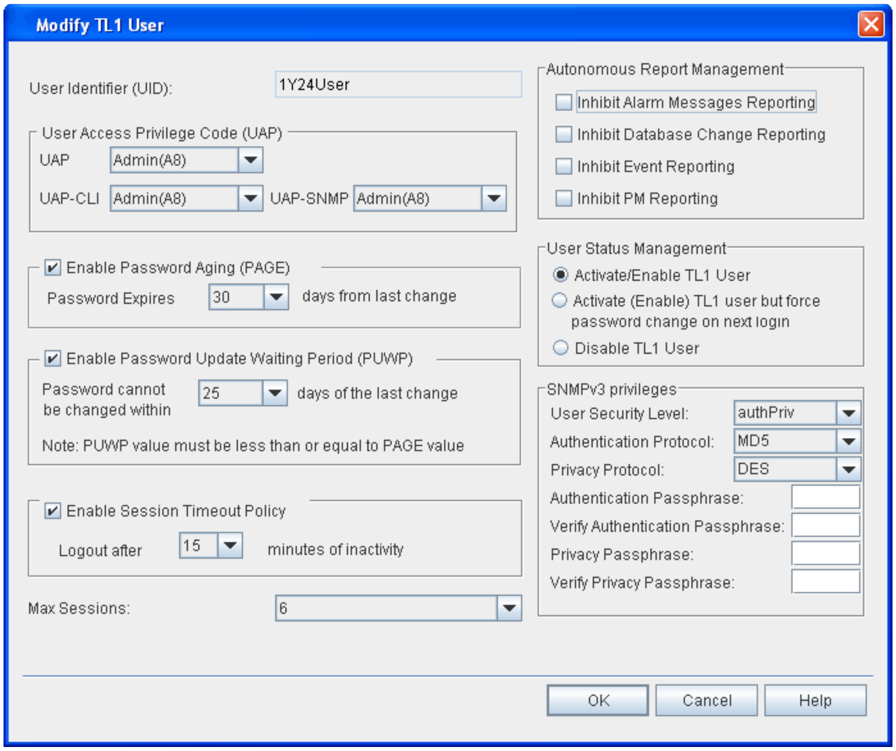
Modifying a TL1 User Profile

5.8 To modify the profile of a TL1 user, click the **Actions** menu, and then click **TL1 User Management**. The **TL1 User Management** dialog box displays. Refer to Figure 5.1, page 15-33.

__ 1. Select the user profile to modify in the **TL1 Users List**.

__ 2. Click **Modify TL1 User**. The **Modify TL1 User** dialog box displays. Refer to Figure 5.4, page 15-41.

Figure 5.4 Modify TL1 User



Modify TL1 User

User Identifier (UID): 1Y24User

User Access Privilege Code (UAP)
UAP: Admin(A8)
UAP-CLI: Admin(A8) UAP-SNMP: Admin(A8)

☑ Enable Password Aging (PAGE)
Password Expires 30 days from last change

☑ Enable Password Update Waiting Period (PUWP)
Password cannot be changed within 25 days of the last change
Note: PUWP value must be less than or equal to PAGE value

☑ Enable Session Timeout Policy
Logout after 15 minutes of inactivity

Max Sessions: 6

Autonomous Report Management
□ Inhibit Alarm Messages Reporting
□ Inhibit Database Change Reporting
□ Inhibit Event Reporting
□ Inhibit PM Reporting

User Status Management
● Activate/Enable TL1 User
○ Activate (Enable) TL1 user but force password change on next login
○ Disable TL1 User

SNMPv3 privileges
User Security Level: authPriv
Authentication Protocol: MD5
Privacy Protocol: DES
Authentication Passphrase:
Verify Authentication Passphrase:
Privacy Passphrase:
Verify Privacy Passphrase:

__ 3. The **User Access Privilege Code (UAP)** area contains drop-down boxes to set the UAP for system privileges and for CLI privileges.

In the **UAP** drop-down box, select the access privilege code for the user.

The user access privilege code (UAP) represents the functional group and authorization level assigned each Craft Station user. The UAP indicates what actions the user can execute. The UAPs and associated system privileges are:

- Administrator or Admin (A8)
- Operator (A7)
- Provisioning (A6)
- Test (A4)
- Public (A2)
- Block CLI (A0)

A8 is the highest user level, and A2 is the lowest. The A8 user can perform all Craft Station actions. The A7 user can administer all TL1 commands excluding security commands, user account administration, and digital certificate administration. The A6 user can perform all Craft Station actions except for setting system and user security and administering user accounts. The A4 user can provision, cancel, and release system elements. The A2 user can edit his or her own password, cancel actions, and view dialog boxes. The A0 user cannot use the CLI cut-through feature to control packet operations or access the SNMP interface. All users can receive autonomous messages as defined by the system administrator.

In the **UAP-CLI** drop-down box, select the access privilege code for the user.

The user access privilege code-command line interface (UAP-CLI) represents the functional group and authorization level assigned each Craft Station user for the CLI cut-through. The UAP-CLI indicates what actions the user can execute. The UAP-CLIs and associated system privileges are:

- Operator (A7)
- Provisioning (A6)
- Test (A4)
- Public (A2)
- Block CLI (A0)

A7 is the highest user level, and A2 is the lowest. The A7 user can administer all CLI commands excluding security commands, user account administration, and digital certificate administration. The A6 user can perform all CLI actions except for setting system and user security and administering user accounts. The A4 user can provision, cancel, and release system elements. The A2 user can edit command their own password, cancel actions, and retrieve information. The A0 user cannot use the CLI cut-through feature to control packet operations. All users can receive autonomous messages as defined by the system administrator.

In the **UAP-SNMP** drop-down box, select the access privilege code for the user.

The user access privilege code-simple network management protocol (UAP-SNMP) represents the functional group and authorization level assigned each Craft Station user for SNMP. The UAP-SNMP indicates what actions the user can execute. The UAP-SNMPs and associated system privileges are:

- Administrative (A8)
- Public (A2)
- Block SNMP (A0)

The A8 user has full read and write access to all SNMP MIBs.The A2 user has full read-only and notify access to the MIBs, and write access to change the user's own SNMP passphrase. The A0 user is blocked from accessing the SNMP interface.

__ 4. Select or deselect the box beside **Enable Password Aging (PAGE)**. If you select the box, click the number of days until the password expires from the **Password Expires** drop-down box. The system begins the count from the day the user modifies the password. This field supports any value between **1** and **255** days.

__ 5. Select or deselect the box beside **Enable Password Update Waiting Period (PUWP)**, and select the number of days before the password can be changed. This field defines the number of days that a user must wait before changing their password.

Note: *The PUWP value must be less than or equal to the value selected in the PAGE field (step 6, page 15-36).*

__ 6. Select or deselect the box beside **Enable Session Timeout Policy** to enable system timeout. This field defines the number of minutes the system waits before it times-out based on a period when no system activity is initiated by the user. This field supports any value between **1** and **99** minutes.

__ 7. In the **Autonomous Report Management** box, select the messages that you do not want displayed for this user profile. Click any of the check boxes below to suppress the type of message described:

__ **Inhibit Alarm Messages Reported**: Click this check box to inhibit messages displayed when an alarm condition on the system sets or clears.

__ **Inhibit Database Change Reporting**: Click this check box to inhibit messages displayed when provisioned system settings change or a user performs an external action is to the system, such as inserting a module.

__ **Inhibit Event Reporting**: Click this check box to inhibit messages displayed when a system event occurs. Events include a change in status condition or a system irregularity that is not severe enough to prompt an alarm.

__ **Inhibit PM Reporting**: Click this check box to inhibit messages displayed when user-provisioned performance monitoring parameters report.

__ 8. In the **User Status Management** box, select the status you want to assign this user. Status values are:

__ **Activate/Enable TL1 User**: The user has access to the system when provisioning in this dialog box is complete, and you click the **OK** button.

__ **Activate (Enable) TL1 user but force password change on next login**: The user has access to the system when provisioning in this dialog box is complete, and you click the **OK** button. But, the user must change his or her password the first time they log in.

__ **Disable TL1 User**: The user does not have access to the system.

__ 9. If you set the UAP SNMP privilege to A2 or A8 in step 3, page 15-41 the SNMPv3 privileges area becomes active. Select the SNMPv3 protocol options by performing the following steps. Otherwise, go to step 10, page 15-44.

__ 9.1 Click the **User Security Level** drop-down box to select **authPriv** (authorization and privacy), **authNoPriv** (authorization but no privacy), or **noAuthnoPriv** (no authorization and no privacy).

__ 9.2 Click the **Authentication Protocol** drop down box to select **MD5** or **SHA**.

__ 9.3 Select the **Privacy Protocol** drop down box to select **DES**.

__ 9.4 Type the authentication passphrase in the **Authentication Passphrase** box. This parameter is mandatory if the user security level is authPriv.

__ 9.5 Type the authentication passphrase in the **Verify Authentication Passphrase** box.

__ 9.6 Type the privacy passphrase in the **Privacy Passphrase** box. This parameter is mandatory if the user security level is authPriv.

__ 9.7 Type the privacy passphrase in the **Verify Privacy Passphrase** box.

__ 10. Click the **Max Sessions** drop-down box to select the maximum number of sessions allows for a user (**1**–**128**, default is **6**).

__ 11. Click **OK** or **Cancel**.

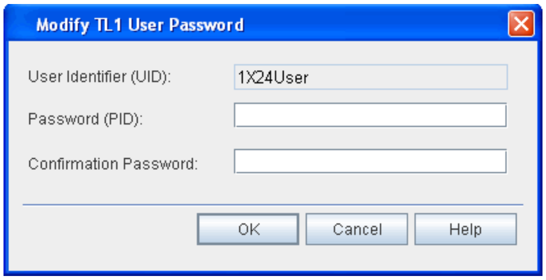
Changing a TL1 User Password

5.9 To change the password of a TL1 user, click the **Actions** menu, then click **TL1 User Management**. The **TL1 User Management** dialog box displays. Refer to Figure 5.1, page 15-33.

__ 1. Select a user in the **TL1 Users List**.

__ 2. Click **Modify TL1 Password**. The **Modify TL1 Password** dialog box displays, showing the user identification of the user selected in step 1, page 15-44. Refer to Figure 5.5, page 15-44.

Figure 5.5 Modify TL1 User Password



Modify TL1 User Password

User Identifier (UID): 1X24User

Password (PID):

Confirmation Password:

__ 3. Type a new password in the **Password (PID)** box.

__ 4. Retype the new password in the **Confirmation Password** box.

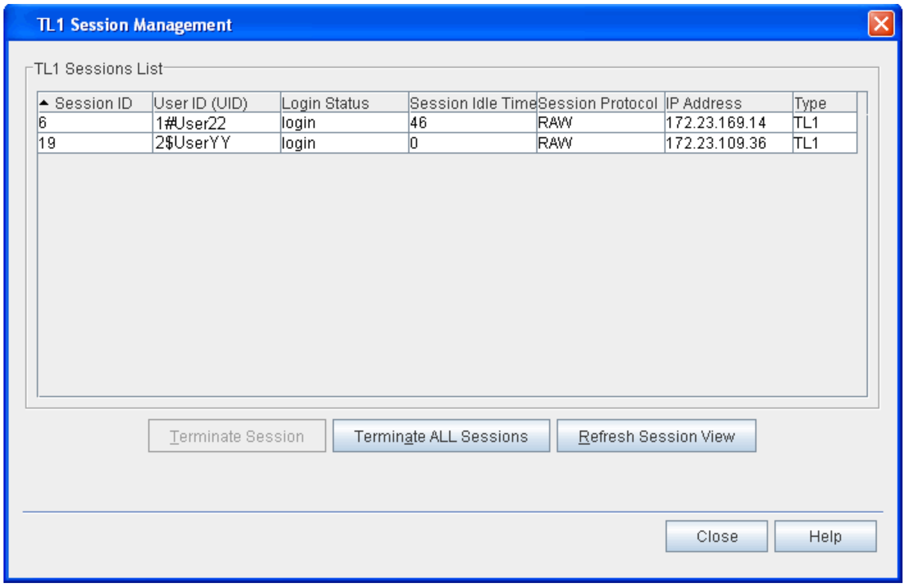
__ 5. Click **OK**. An Information box displays confirming the password change was effective.

Session Management

5.10 A Craft Station user with A8 (Admin privileges) can view or terminate current TL1 sessions by accessing the **TL1 Session Management** dialog box. Access the **TL1 Session Management** dialog box by performing the following steps:

__ 1. Right-click the NE icon in the **Navigation Window** to view the shortcut menu, then click **TL1 Session Management**. The **TL1 Session Management** dialog box displays. Refer to Figure 5.6, page 15-45.

Figure 5.6 TL1 Session Management



Session ID	User ID (UID)	Login Status	Session Idle Time	Session Protocol	IP Address	Type
6	1#User22	login	46	RAW	172.23.169.14	TL1
19	2$UserYY	login	0	RAW	172.23.109.36	TL1

5.11 The **TL1 Session Management** dialog box provides the following information about sessions on this NE:

- Session ID: unique identifier of the session that the user is logged in to.
- User ID (UID): ID of session user
- Login Status: identifies if any user is currently logged into a session
  - login
  - notlogin
- Session Idle Time: length of time a session has been idle (seconds)

- Session Protocol: identifies the protocol used to start the session
    - TELNET
    - RAW
    - SERIAL
- IP Address: IP address associated with this session
- Type: TL1

Terminating a Session

5.12 At the **TL1 Session Management** dialog box, a user with administrator privileges can terminate one or all sessions.

Terminating a Single Session

5.13 Terminate a specific session by performing the following steps:

__ 1. Click the session to delete in the **TL1 Sessions List** area.

__ 2. Click **Terminate Session**. Refer to Figure 5.6, page 15-45.

__ 3. A **Confirmation** box displays requesting confirmation that you want to continue with the termination.

__ 4. Click **OK** or **Cancel**.

Terminating All Sessions

5.14 Terminate all sessions by performing the following steps:

__ 1. In the **TL1 Session Management** dialog box, click **Terminate ALL Sessions**. Refer to Figure 5.6, page 15-45.

__ 2. A **Confirmation** box displays requesting confirmation that you want to continue with the terminations.

__ 3. Click **OK** or **Cancel**.

Refreshing Session View

5.15 Use the **Refresh Session View** button to confirm the list of sessions in the **TL1 Sessions List** box is current. Refresh the list by performing the following steps:

__ 1. In the **TL1 Session Management** dialog box, click **Refresh Session View**. Refer to Figure 5.6, page 15-45.

__ 2. A multi-colored refresh bar displays briefly in the lower right corner of the screen, indicating the NE is retrieving session data. When this bar disappears, the refresh is complete, and the list is current.

Retrieving TL1 Logs

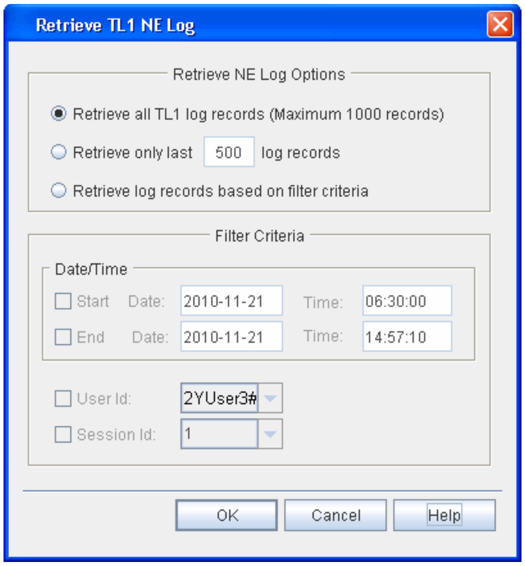
5.16 Retrieve log records in the TL1 log file of a specific NE using the **Retrieve TL1 NE Log** selection under the NE icon in the **Navigation Window**. This log captures all TL1 command requests and responses on all resources that are accessible by a user. This log includes creation, deletion and modification of entities; software and database management activities; all security related events such as user log in, account creation, account modification, and modification of system security policies. This log file is accessible to users with Admin privileges (A8) only.

5.17 Each NE stores a maximum of 1000 log records. A log record can be a TL1 command, a TL1 command response, or TL1 event message related to security. Filter the log by time, session, user ID, or number of records. If you do not select a filter, all records in the log file display.

5.18 Access the **Retrieve TL1 NE Log** dialog box by performing the following steps:

__ 1. Right-click the NE icon in the **Navigation Window** to view the shortcut menu, then click **Retrieve TL1 NE Log**. The **Retrieve TL1 NE Log** dialog box displays. Refer to Figure 5.7, page 15-47.

Figure 5.7 Retrieve TL1 NE Log



Retrieve TL1 NE Log

Retrieve NE Log Options

● Retrieve all TL1 log records (Maximum 1000 records)

○ Retrieve only last 500 log records

○ Retrieve log records based on filter criteria

Filter Criteria

Date/Time

□ Start Date: 2010-11-21 Time: 06:30:00

□ End Date: 2010-11-21 Time: 14:57:10

□ User Id: 2YUser3#

□ Session Id: 1

__ 2. In the **Retrieve TL1 NE Log** box, click one of the following options to define the number of logs to retrieve:

- Retrieve all TL1 log records.
- Retrieve a specific number of the last records set.
- Retrieve records based on filtering. Refer to step 3, page 15-48.

__ 3. In the **Filter Criteria** box, click any following options for filtering:

- Click a **Start Date** by day and time. Click an **End Date** by day and time. To capture records through the current date and time, leave the **End** field unchecked.
- Click a specific **User Id** from the drop-down box to filter on users.
- Click a **Session Id** from the drop-down box to filter on a specific session.

__ 4. Click **OK** to start the report.

__ 5. The **Retrieve TL1 NE Logs** report displays. Logs display in two categories:

- Click the **Commands** tab to view TL1 commands.
- Click the **Events** tab to view system events.

__ 6. Click **OK** or **Cancel**.

Retrieving AO Logs

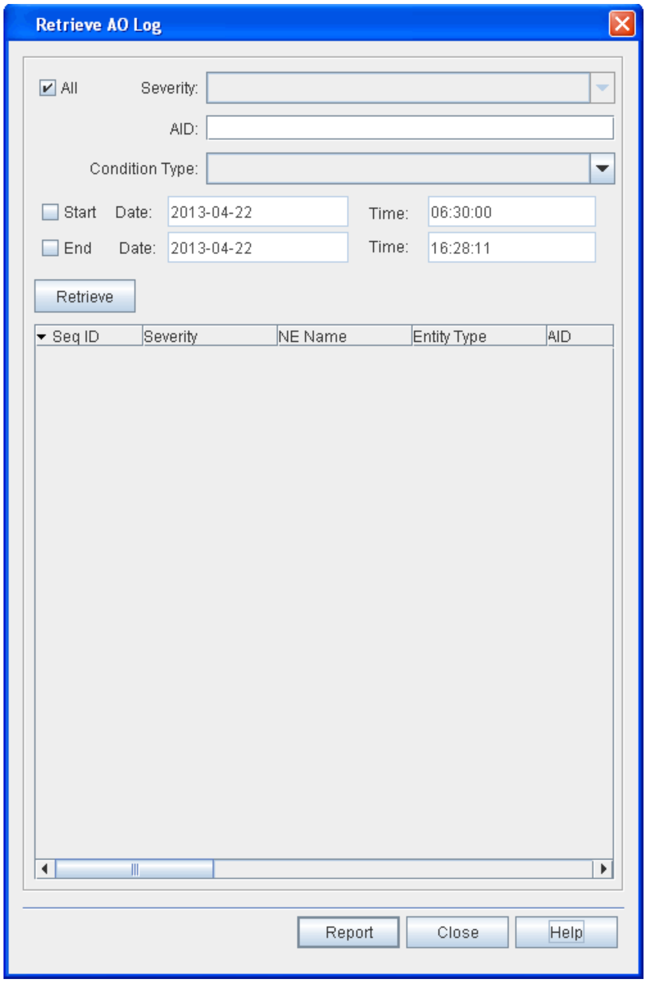
5.19 Retrieve log records in the AO log file of a specific NE using the **Retrieve AO Log** selection under the NE icon in the **Navigation Window**.

5.20 Use the RTRV-AO command to retrieve copies of Autonomous Output messages that are suspected as missing or for other verification purposes. Up to 1000 autonomous messages are stored in the NE. Examples of autonomous messages are REPT^DBCHG, REPT^ALM, and REPT^ EVT. The autonomous messages retrieved by RTRV-AO are listed in ATAG or DBCHSEQ order in the output. If none of the available autonomous messages on the system satisfy the specific selection criteria, then a complete normal response is issued.

5.21 Access the **Retrieve TL1 NE Log** dialog box by performing the following steps:

__ 1. Right-click the NE icon in the **Navigation Window** to view the shortcut menu, then click **Retrieve AO Log**. The **Retrieve AO Log** dialog box displays. Refer to Figure 5.8, page 15-49.

Figure 5.8 Retrieve TL1 NE Log



☑ All Severity:

AID:

Condition Type:

□ Start Date: 2013-04-22 Time: 06:30:00

□ End Date: 2013-04-22 Time: 16:28:11

__ 2. Choose one of the following options:

- Click the **Severity** drop-down box to select **CR**, **MJ**, **MN**, or **CL**.
- Or click the **All** box to select all severity levels.

__ 3. In the **AID** box, type an access identifier (AID) by to filter the autonomous output.

__ 4. Click the **Condition Type** drop-down box to select a condition type by which to filter the autonomous output.

__ 5. Perform the following steps to filter the autonomous output by day and time:

- Click the **Start** box. In the **Date** box type the date in the format YYYY-MM-DD. In the **Time** box type the time in the format HH-MM-SS. To capture records through the current date and time, leave the **End** box unchecked.
- Click the **End** box. In the **Date** box type the date in the format YYYY-MM-DD. In the **Time** box type the time in the format HH-MM-SS.

__ 6. Click **Retrieve** to retrieve the autonomous output.

__ 7. (Optional) Click Report to generate an autonomous output report.

__ 8. The **Retrieve TL1 NE Logs** report displays. Logs display in two categories:

- Click the **Commands** tab to view TL1 commands.
- Click the **Events** tab to view system events.

__ 9. Click **OK** or **Cancel**.

6. System Administration

6.1 This section provides instructions for managing the NE database, upgrading the NE, provisioning DHCP, managing IP security, and setting system date and time.

Note: *Refer to TL1 Command Reference Manual for additional details on system settings. Click the Help menu in the Craft Station to access this document.*

IPSec Management

6.2 The Craft Station offers IPSec security to protect communication between the Craft Station and the NE, and between all NEs deployed in a gateway application. IPSec is an IP-layer protocol configured at the operating system level in the IP stack. On the mTera NE with proxy mode disabled, IPsec can be enabled on SEIM interfaces, DCN IPPG, or GCC interfaces.

6.3 This section describes how to implement IPsec security between the system processor module of the NE, the Craft Station, and the PC supporting it.

6.4 The IPSec feature provisions inbound and outbound security policies in the security policy database (SPD), defining for the NE the range of destination addresses and the range of source addresses allowed. The system administrator (A8) manages and configures application levels of the SPD and how it is accessed.

Note 1: *Confirm the Certificate/Key has been downloaded to the NE before beginning. The IPSec feature must be set up correctly at both the NE and the PC running the Craft Station or communication may be disrupted between the two.*

Note 2: *For more detailed information on the IP Security feature, refer to System Administration Using Management Systems and TL1 Command Reference Manual.*

Setting Up IPSec on the PC with Digital Certificates

6.5 Configure the PC running the Craft Station software for IP security before provisioning the IPSec feature in the Craft Station. This section provides the procedure for configuring the PC using digital certificates.

Note: *Administrator privileges on the PC are required to complete this procedure.*

Importing the Root Trusted Certificate

6.6 Add the root certificate to the trusted certificates folder by performing the following steps:

__ 1. On the Windows desktop, click the **Start** button, then click **Run**.

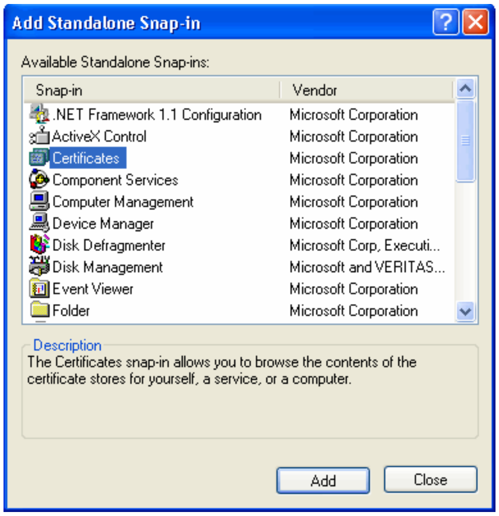
__ 2. In the **Run** dialog box, type **mmc** in the **Open** box.

__ 3. Click **OK**, and the **Console** dialog box displays.

__ 4. From the **File** menu, click **Add/Remove Snap-in**.

__ 5. Click **Add**. The **Add Standalone Snap-in** dialog box displays. Refer to Figure 6.1, page 15-52.

Figure 6.1 Add Standalone Snap-In



Add Standalone Snap-in

Available Standalone Snap-ins:

Snap-in	Vendor
.NET Framework 1.1 Configuration	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Microsoft Corp, Executi...
Disk Management	Microsoft and VERITAS...
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation

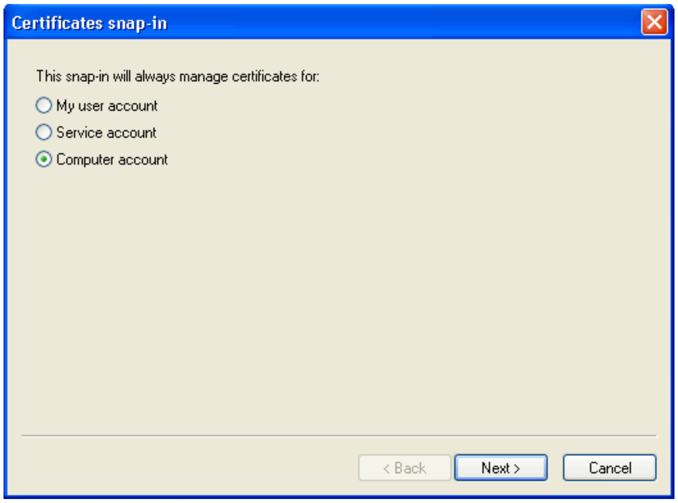
Description

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

__ 6. Select **Certificates** from the list, and click **Add**. The **Certificates Snap-in** dialog box displays.

__ 7. Click **Computer account**. Click **Next**. Refer to Figure 6.2, page 15-52.

Figure 6.2 Certificates Snap-In



Certificates snap-in

This snap-in will always manage certificates for:

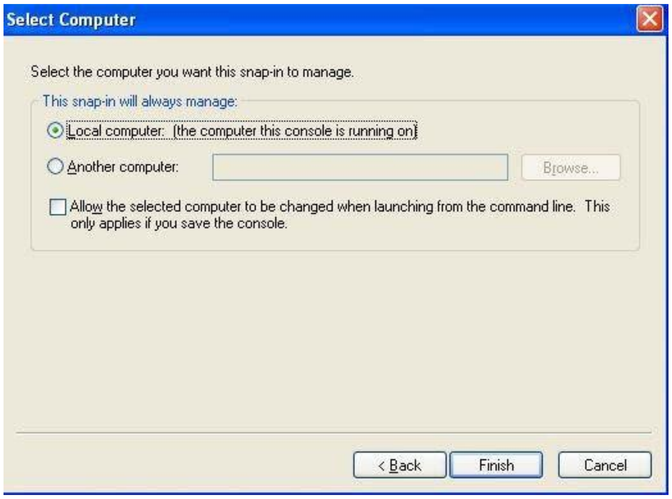
○ My user account

○ Service account

● Computer account

__ 8. At the next dialog box, click **Local Computer**. Refer to Figure 6.3, page 15-53.

Figure 6.3 Select Local Computer



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

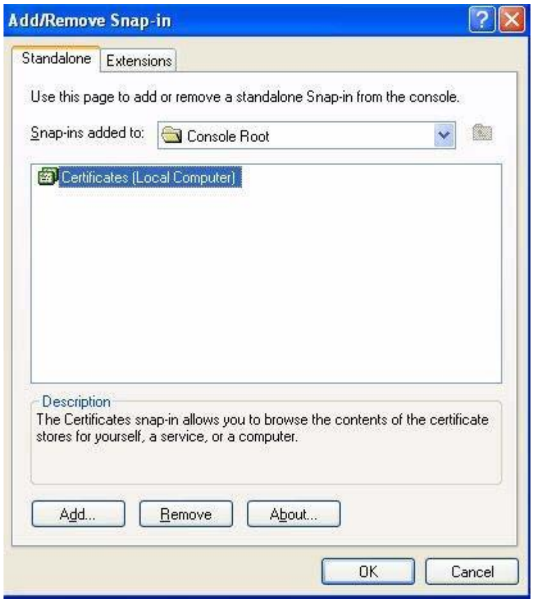
● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

__ 9. Click **Finish**. A dialog box similar to the one shown in Figure 6.4, page 15-53, displays.

Figure 6.4 Certificates on Local Computer



Add/Remove Snap-in

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Certificates (Local Computer)

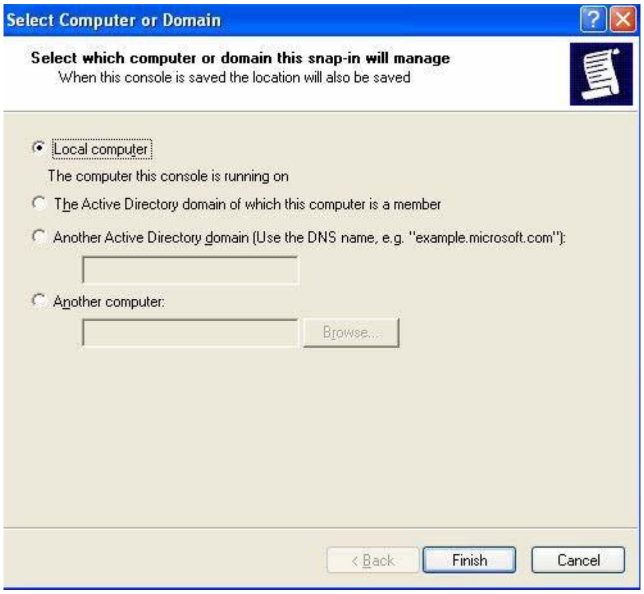
Description

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

__ 10. Click **OK**. The **Add Standalone Snap-in** dialog box displays.

__ 11. Scroll down, click **IP Security Policy Management**, then click the **Add** button. A dialog box similar to the one shown in Figure 6.5, page 15-54 displays.

Figure 6.5 Select Local Computer



Select Computer or Domain

Select which computer or domain this snap-in will manage
When this console is saved the location will also be saved

● Local computer
The computer this console is running on
○ The Active Directory domain of which this computer is a member
○ Another Active Directory domain (Use the DNS name, e.g. "example.microsoft.com"):
○ Another computer:

__ 12. Click **Local computer**, then click **Finish**. The **Add Standalone Snap-in** dialog box displays.

__ 13. Click **IP Security Monitor**, then click **Add**.

__ 14. Click the **Close** button in the **Add/Remove Snap-in**.

__ 15. Click **OK**.

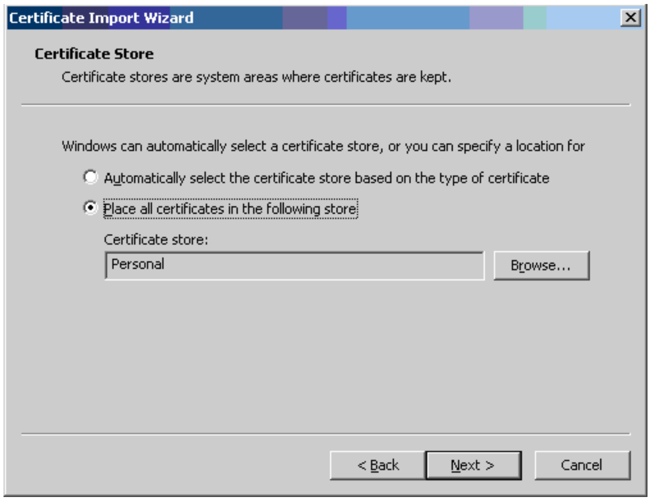
__ 16. In the **Console** dialog box, expand **Certificates**. Right-click **Personal** to view the shortcut menu, point to **All Tasks**, then click **Import**.

__ 17. The **Certificate Import Wizard** launches. In the first screen, **Browse** to the file that contains your root certificate. Click **Next**.

__ 18. The **Password** dialog box displays. Type the password for accessing the keys in the file. Click **Next**.

__ 19. The **Certificate Store** dialog box displays. In this screen, define system locations in which to store the certificates. Click **Place all certificates in the following store**. Refer to Figure 6.6, page 15-54.

Figure 6.6 Store Certificate



Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate
● Place all certificates in the following store

Certificate store:
Personal

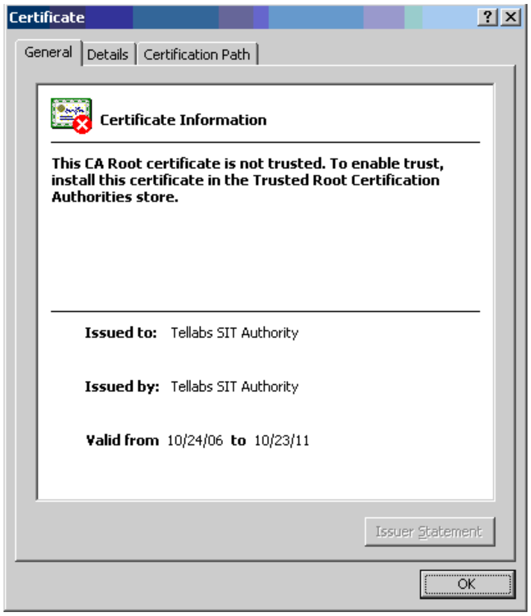
__ 20. Click the **Browse** button, and select **Personal**. Click **Next**.

__ 21. A summary screen displays describing the settings for certificate storage. Click **Finish** to accept all settings.

__ 22. In the **Console** dialog box, expand **Certificates (Local Computer)**, click **Personal**, then click **Certificates**. The certificates just created display in the right window.

__ 23. Right-click one of the certificates to view the shortcut menu, then click **Properties**. The **Properties** dialog box displays. Refer to Figure 6.7, page 15-55.

Figure 6.7 Certificate Properties



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Tellabs SIT Authority

Issued by: Tellabs SIT Authority

Valid from 10/24/06 **to** 10/23/11

Note: *The Root Certificate is the one in which the value in the **Issued To** field is the same as the value in the **Issued By** field.*

__ 24. Click **OK** to close the **Properties** dialog box.

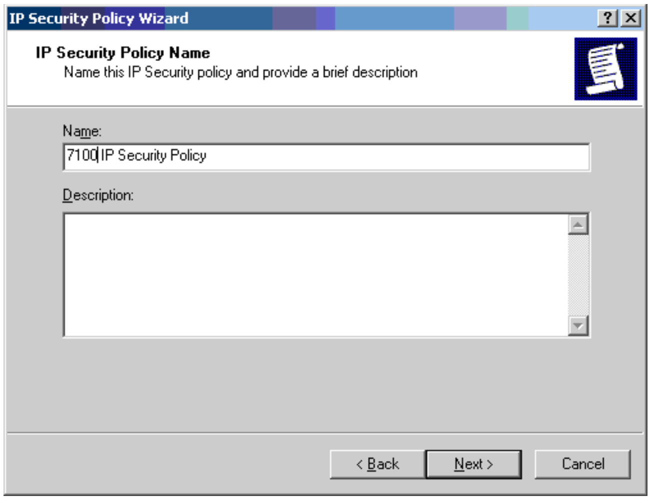
__ 25. In the **Console** dialog box, expand **Certificates (Local Computer)**, then expand **Personal**.

__ 26. Click the root certificate in the right window pane, and drag it to the **Trusted Root Certification Authorities** folder.

__ 27. In the **Console** dialog box, right-click **IP Security Policy on Local Computer** to view the shortcut menu, point to **All Tasks**, then click **Create IP Security Policy**.

__ 28. The **IP Security Policy Wizard** launches. In the first dialog box, type a **Name** for the policy, then click **Next**. Refer to Figure 6.8, page 15-56.

Figure 6.8 IP Security Policy Wizard



IP Security Policy Wizard

IP Security Policy Name

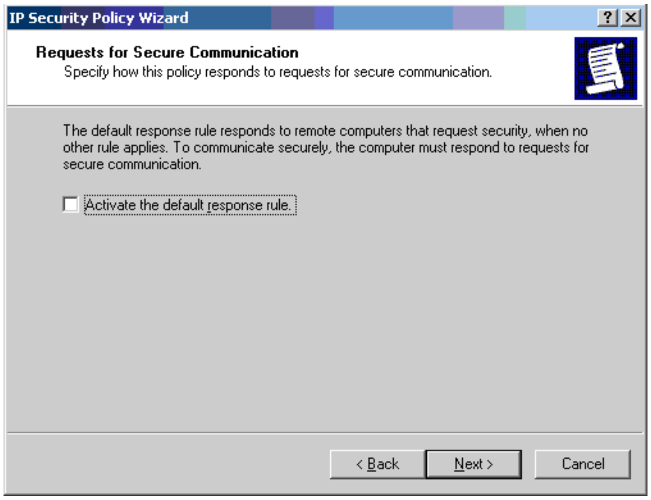
Name this IP Security policy and provide a brief description

Name: 7100 IP Security Policy

Description:

__ 29. In the next dialog box, deselect the box for **Activate the default response rule**. Click **Next**. Refer to Figure 6.9, page 15-56.

Figure 6.9 IP Security Policy Wizard



IP Security Policy Wizard

Requests for Secure Communication

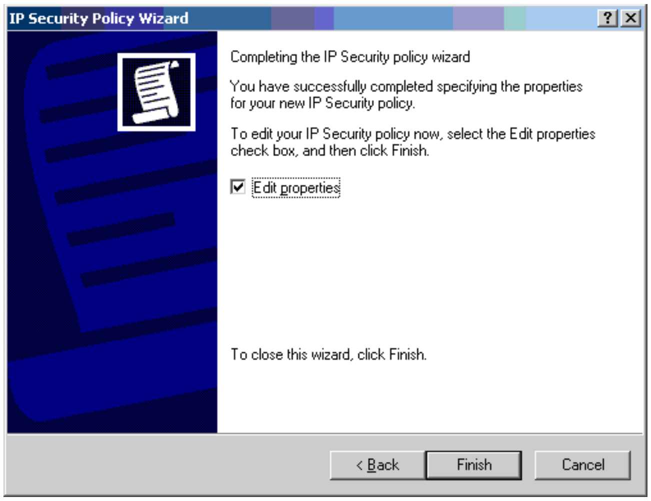
Specify how this policy responds to requests for secure communication.

The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

□ Activate the default response rule.

__ 30. In the next dialog box, click the **Edit properties** check box. Click **Finish**. Refer to Figure 6.10, page 15-57.

Figure 6.10 IP Security Policy Wizard



Completing the IP Security policy wizard

You have successfully completed specifying the properties for your new IP Security policy.

To edit your IP Security policy now, select the Edit properties check box, and then click Finish.

☑ Edit properties

To close this wizard, click Finish.

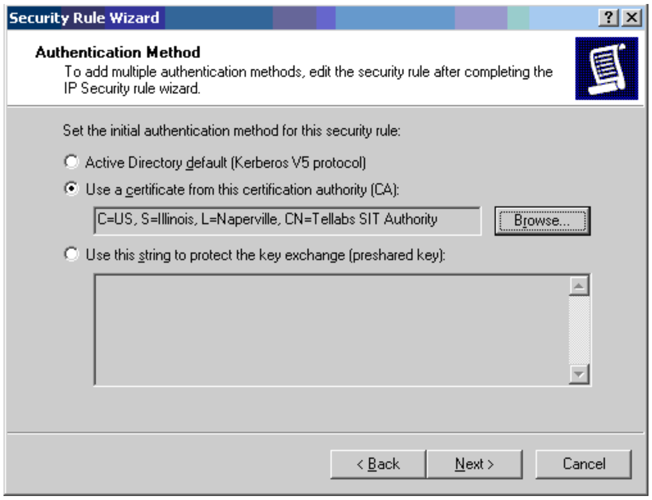
__ 31. When the wizard completes, right-click the policy to view the shortcut menu. Click **Properties** to edit the configuration properties.

__ 32. Configure the filter properties for the new IPsec policy. Click the **Add** button in the **New IP Security Policy Properties** dialog box. The **Security Rule Wizard** launches.

Note: *The rule does not specify a tunnel and should apply to all network connections.*

__ 33. Click **Use a certificate from this certification authority (CA)**. Type the name of the string that identifies the root certificate that was just imported, or click **Browse**. Click **Next**. Refer to Figure 6.11, page 15-57.

Figure 6.11 Define Certificate



Authentication Method

To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.

Set the initial authentication method for this security rule:

○ Active Directory default (Kerberos V5 protocol)

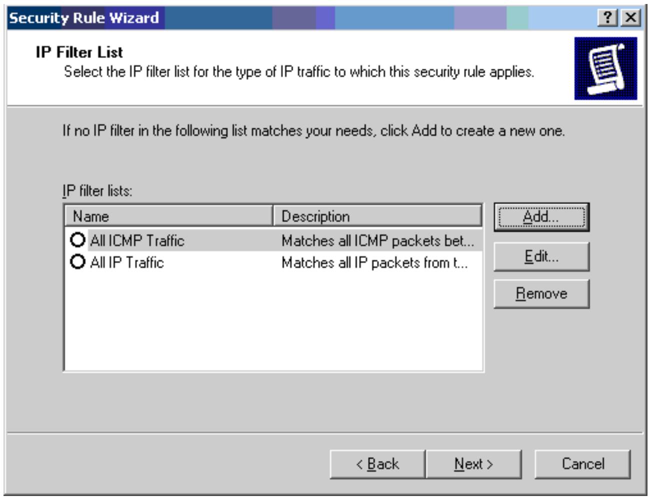
● Use a certificate from this certification authority (CA):

C=US, S=Illinois, L=Naperville, CN=Tellabs SIT Authority

○ Use this string to protect the key exchange (preshared key):

__ 34. The **IP Filter** dialog box displays. Click **Add** to add a new filter. Refer to Figure 6.12, page 15-58.

Figure 6.12 Add Filter



IP Filter List

Select the IP filter list for the type of IP traffic to which this security rule applies.

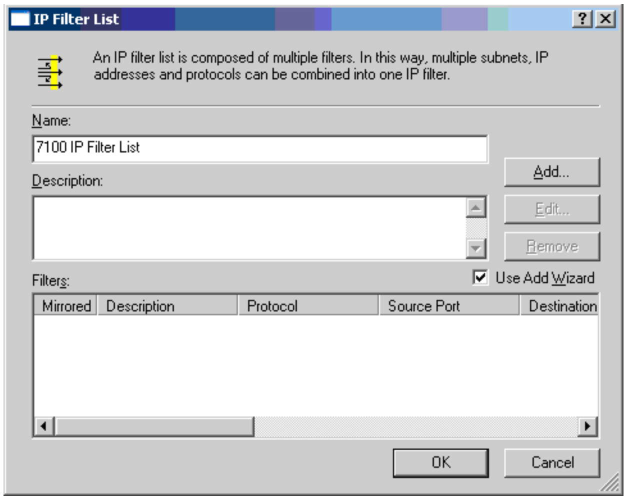
If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...

__ 35. The **IP Filter List** dialog box displays. Type the name of the filter list in the **Name** box. Click **Add**. Click **Next**. Refer to Figure 6.13, page 15-58.

Figure 6.13 IP Filter List



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: 7100 IP Filter List

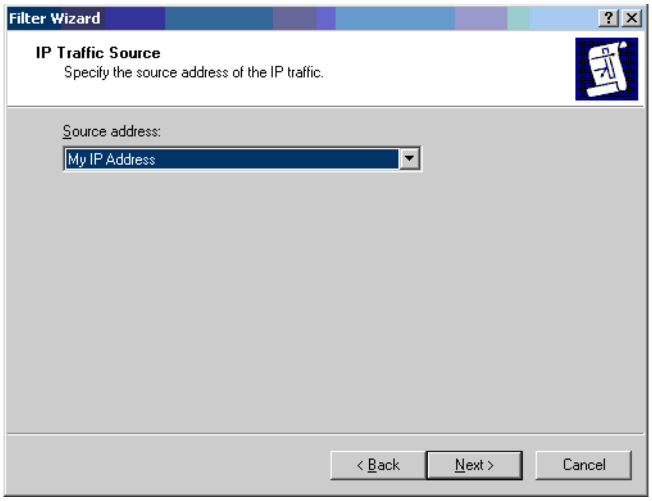
Description:

Filters: ☑ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

__ 36. The **IP Traffic Source** dialog box displays. Type the IP address of the local machine in the **Source Address** box. Click **Next**. Refer to Figure 6.14, page 15-59.

Figure 6.14 IP Traffic Source


Filter Wizard

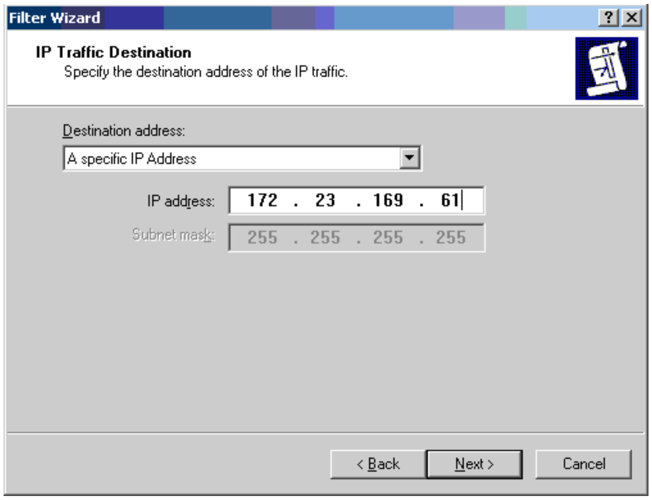
IP Traffic Source

Specify the source address of the IP traffic.

Source address: My IP Address

__ 37. The **IP Traffic Destination** dialog box displays. Type the IP address of the destination (endpoint) machine in the **Destination address** box. Click **Next**. Refer to Figure 6.15, page 15-59.

Figure 6.15 IP Traffic Destination


Filter Wizard

IP Traffic Destination

Specify the destination address of the IP traffic.

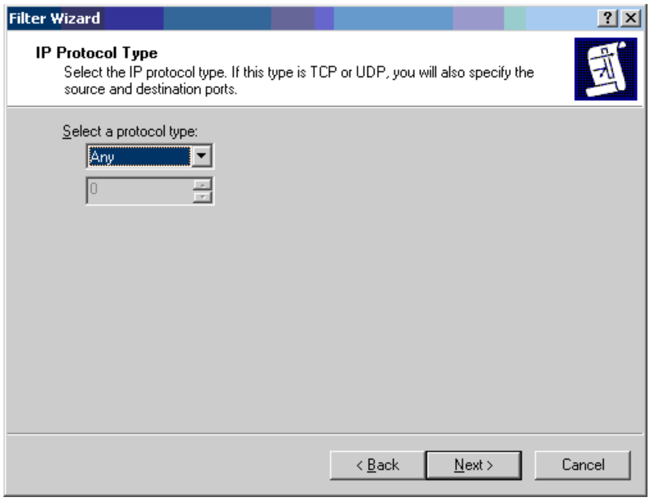
Destination address: A specific IP Address

IP address: 172 . 23 . 169 . 61

Subnet mask: 255 . 255 . 255 . 255

__ 38. The **IP Protocol Type** dialog box displays. Select **Any** from the **Select a protocol type** drop-down box. Click **Next**. Refer to Figure 6.16, page 15-60.

Figure 6.16 IP Protocol Type



IP Protocol Type

Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.

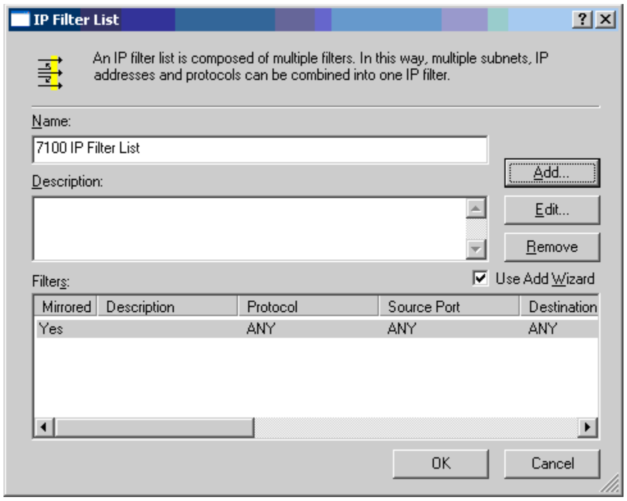
Select a protocol type: Any

0

__ 39. Click **Finish**, and the **Filter Wizard** closes.

__ 40. In the **IP Filter List** dialog box, the new filter displays in the list. Click **OK**. Refer to Figure 6.17, page 15-60.

Figure 6.17 IP Filter List



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: 7100 IP Filter List

Description:

☑ Use Add Wizard

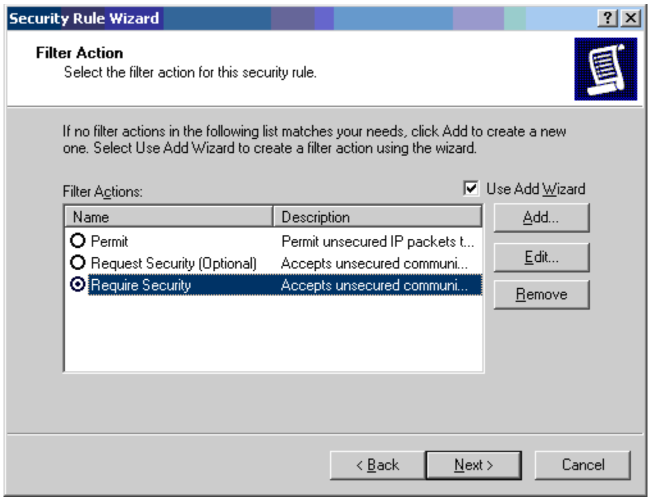
Filters:

Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY

__ 41. In the **Security Rule Wizard**, select the new filter. Click **Next**.

__ 42. In the **Security Rule Wizard**, select **Require Security** as the filter action for the newly created filter. Click **Next**. Refer to Figure 6.18, page 15-61.

Figure 6.18 Filter Action



Filter Action

Select the filter action for this security rule.

If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

Filter Actions:

☑ Use Add Wizard

Name	Description
○ Permit	Permit unsecured IP packets t...
○ Request Security (Optional)	Accepts unsecured communi...
● Require Security	Accepts unsecured communi...

__ 43. Click **Next**, then click **Finish**. The **Security Rule Wizard** closes.

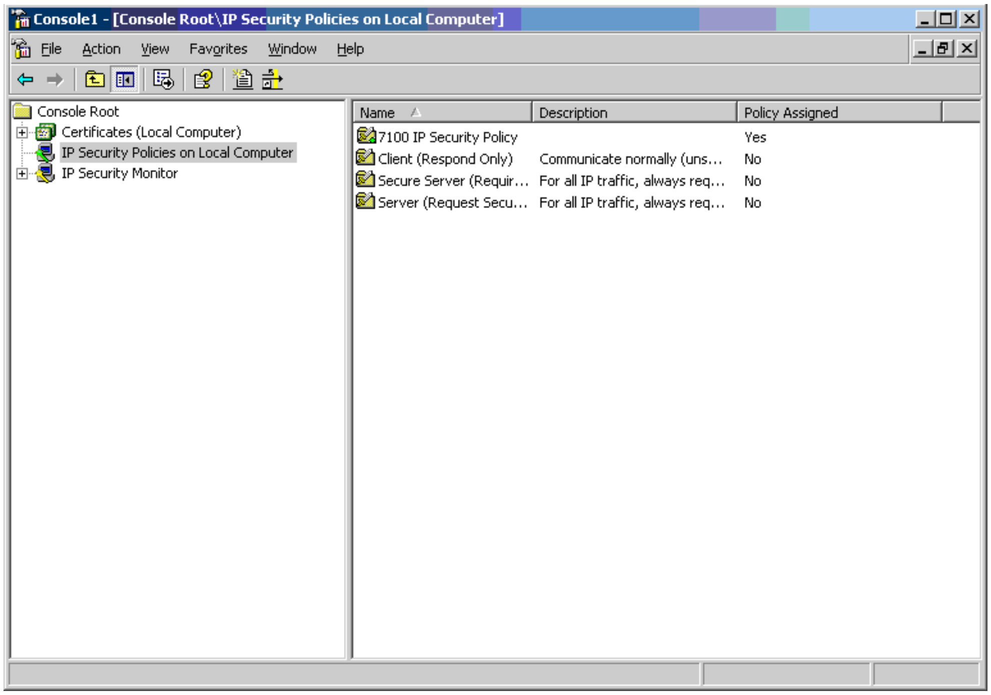
__ 44. In the **Local Security Settings** dialog box, click the policy to select it. Refer to Figure 6.19, page 15-62.

Note: *Before completing the next step, confirm the NE is configured to allow IPSec. If the NE is not configured, step 45, page 15-61 may interrupt communication with the NE.*

__ 45. From the **Action** menu, click **Assign.** This step enables IP Security on the PC.

Note: *If the security policy does not activate, start IPSec and Cryptograph services in Windows. Access Admin tools, and open Services manager.*

Figure 6.19 Local Security Settings


Console1 - [Console Root\IP Security Policies on Local Computer]
File
Action
View
Favorites
Window
Help

Console Root
Certificates (Local Computer)
IP Security Policies on Local Computer
IP Security Monitor

Name	Description	Policy Assigned
7100 IP Security Policy		Yes
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No

Provisioning IPSec on the NE

6.7 This section describes how to provision IP Security features on the NE via the Craft Station software.

Certificates

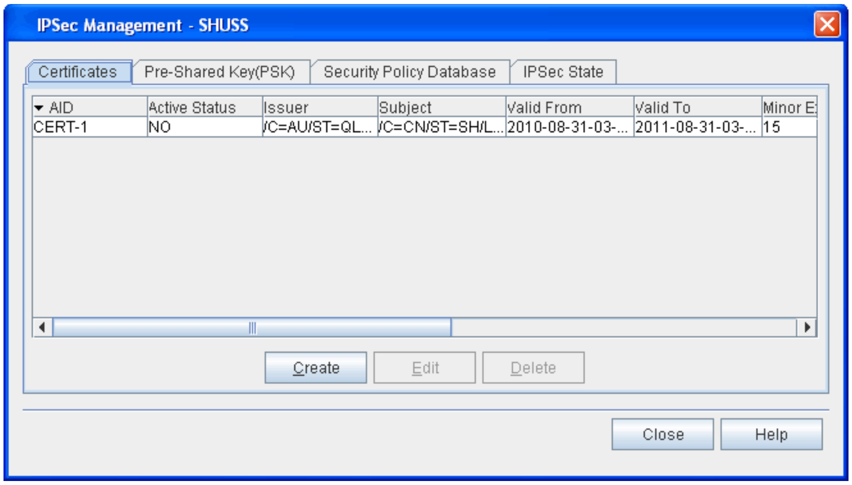
6.8 Download and install the IPSec certificate or key (PKCS12 files and PSK files) to the NE by performing the following steps:

Note 1: *IPSec should be disabled on the PC until the NE is ready for IPSec connection.*

Note 2: *The certificates and keys are downloaded to a hidden location that is not visible.*

__ 1. In the **Navigation Window**, right-click the NE icon to view the shortcut menu, then click **IPSec Management**. The **IPSec Management** dialog box displays. Refer to Figure 6.20, page 15-63.

Figure 6.20 IPSec Management

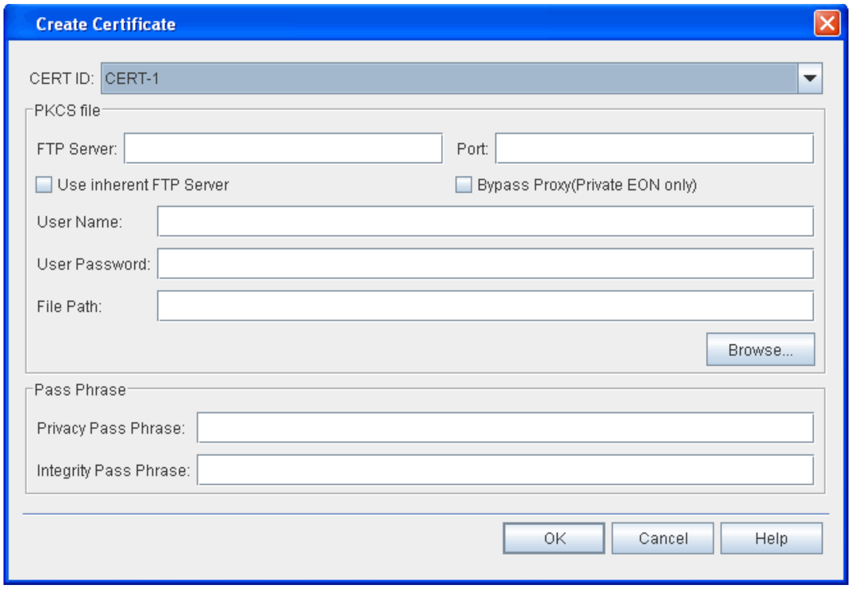


AID	Active Status	Issuer	Subject	Valid From	Valid To	Minor E:
CERT-1	NO	/C=AU/ST=QL...	/C=CN/ST=SH/L...	2010-08-31-03-...	2011-08-31-03-...	15

__ 2. In the **IPSec Management** dialog box, verify that the **Certificates** tab is selected.

__ 3. Click **Create**. The **Create Certificate** dialog box displays. Refer to Figure 6.21, page 15-63.

Figure 6.21 Create Certificate



CERT ID: CERT-1

__ 4. Click the **CERT ID** drop-down box to select the certificate ID number (**CERT-1** or **CERT-2**). You can install a maximum of two certificates on an NE, but the certificates cannot be active simultaneously.

__ 5. Complete the following information in the **PKCS file** area:

__ 5.1 If the digital certificate is on the PC, click the **Use inherent FTP Server** box. The Craft Station provides an inherent **FTP** server for file transfers to the NE. An FTP server may also be running on the PC (refer to Setting Up FTP, page 15-12).

__ 5.2 Leave the **Bypass Proxy (Private EON only)** box unchecked.

__ 5.3 If necessary, type the IP address of the FTP server in the **FTP Server** box.

__ 5.4 If necessary, type the logical port number associated with the Host Machine IP address in the **Port** box.

__ 6. In the **User Name** box, type the name of the user with FTP server rights.

__ 7. In the **User Password** box, type the password associated with the **User Name**.

__ 8. Use the **Browse** button to select the file path, or type the file path where the security files will be stored in the **File Path** box.

__ 9. Complete the following information in the **Pass Phrase** area:

__ 9.1 In the **Privacy Pass Phrase** box, type the privacy pass phrase for the PKCS#12 file (**8**–**32** characters).

__ 9.2 In the **Integrity Pass Phrase** box, type the privacy pass phrase for the PKCS#12 file (**8**–**32** characters).

__ 10. Click **OK**.

Modifying IPSec Certificates

6.9 By using digital certificates, the Craft Station monitors the IP addresses of NEs allowed to participate in the Internet Key Exchange. When a certificate is loaded, the IP addresses contained in the file are stored and can be displayed.

6.10 Modify the state of a certificate by performing the following steps:

__ 1. In the **Navigation Window**, right-click the NE icon to view the shortcut menu, then click **IPSec Management**. The **IPSec Management** dialog box displays.

__ 2. Verify that the **Certificates** tab is selected.

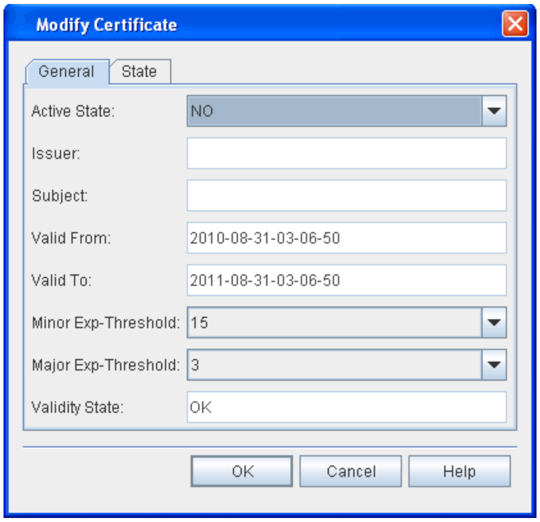
__ 3. Click to highlight the target certificate.

__ 4. Click **Edit**. The **Modify Certificate** dialog box displays.

General Tab

__ 5. Verify that the **General** tab is selected. Refer to Figure 6.22, page 15-65.

Figure 6.22 Modify Certificate



Active State: NO

Issuer:

Subject:

Valid From: 2010-08-31-03-06-50

Valid To: 2011-08-31-03-06-50

Minor Exp-Threshold: 15

Major Exp-Threshold: 3

Validity State: OK

__ 6. Verify the following information:

- **Issuer** (information about the issuer of the digital certificate)
- **Subject** (information about the digital certificate)
- **Valid From** (date from which the digital certificate is valid, year-month-day-hour-minute-second)
- **Valid To** (date to which the digital certificate is valid, year-month-day-hour-minute-second)
- **Validity State** (OK, INVALID, EXPIRING, EXPIRING SOON, EXPIRED)

__ 7. Click the **Active State** drop-down box to specify if the certificate will be active (**NO** or **YES**). When you set a digital certificate to active, the system automatically sets the other digital certificate to inactive.

__ 8. Click the **Minor Exp-Threshold** drop-down box to specify a first threshold indicating the number of remaining days for which the current certificate is still valid (**0**–**365**, default is 15 days, configure to 0 to disable parameter). When this threshold is crossed, the Validity State transitions to "EXPIRING" and the system generates an event.

__ 9. Click the **Major Exp-Threshold** drop-down box to specify the second threshold indicating the number of remaining days for which the current certificate is still valid (**0**–**365**, default is 3 days, configure to 0 to disable parameter). When this threshold is crossed, the Validity State transitions to "EXPIRING SOON" and the system generates an event. Configure the Major Exp-Threshold to a value less than or equal to the value of the Minor Exp-Threshold.

State Tab

_ 10. Click the **State** tab.

__ 11. In the **Management Command** area, click **In-Service (IS)** or **Out-Of-Service (OOS)**.

__ 12. Click **OK**.

Deleting Certificate

6.11 Delete a certificate by performing the following steps:

__ 1. In the **Navigation Window**, right-click the NE icon to view the shortcut menu, then click **IPSec Management**. The **IPSec Management** dialog box displays.

__ 2. Verify that the **Certificates** tab is selected.

__ 3. Click to highlight the target certificate.

__ 4. Click **Delete**. A **Confirmation** box displays asking if you want to delete the certificate.

__ 5. Click **OK**.

Pre-Shared Key

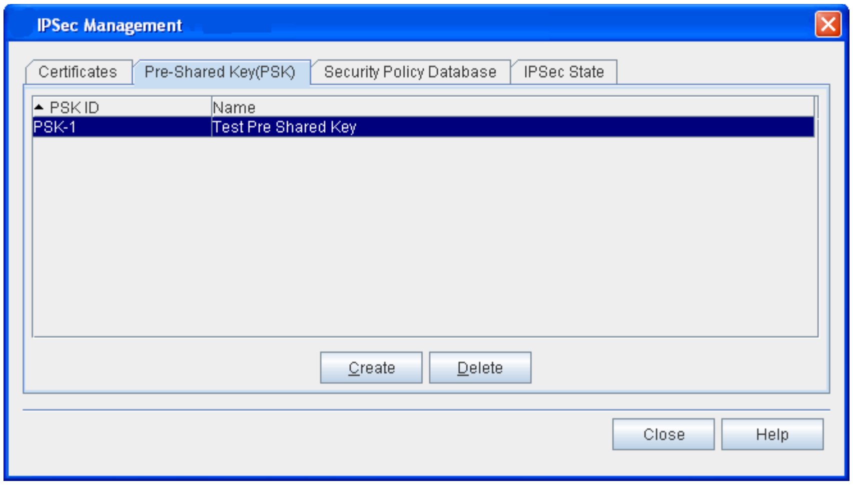
6.12 A pre-shared key authorizes a particular entity with an IP address connected to the DCN (Data Communication Network) to participate in IKE (Internet Key Exchange) with a network element using this Pre-Shared Key (PSK).

6.13 Create a PSK by performing the following steps:

__ 1. In the **Navigation Window**, right-click the NE icon to view the shortcut menu, then click **IPSec Management**. The **IPSec Management** dialog box displays.

__ 2. Click the **Pre-Shared Key (PSK)** tab. Refer to Figure 6.23, page 15-66.

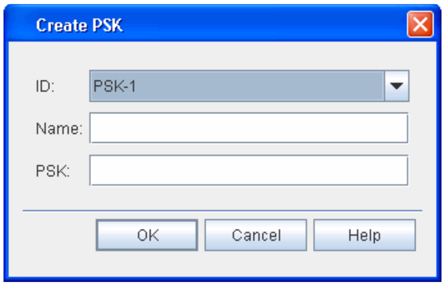
Figure 6.23 Pre-Shared Key (PSK)



PSK ID	Name
PSK-1	Test Pre Shared Key

__ 3. Click **Create**. The **Create PSK** dialog box displays. Refer to Figure 6.24, page 15-67.

Figure 6.24 Create PSK



Create PSK

ID: PSK-1

Name:

PSK:

__ 4. Click the **ID** drop-down box to select the PSK ID. The system supports 1000 pre-shared keys (**PSK-1**–**PSK-1000**).

__ 5. Type a name for the PSK in the **Name** box (0–47 character string).

__ 6. In the **PSK** box, type the pre-shared key (16 character or 64–128 character ASCII or HEX character string).

__ 7. Click **OK**.

Deleting Pre-Shared Key

6.14 Delete a pre-shared key by performing the following steps:

__ 1. In the **Navigation Window**, right-click the NE icon to view the shortcut menu, then click **IPSec Management**. The **IPSec Management** dialog box displays.

__ 2. Click the **Pre-Shared Key (PSK)** tab.

__ 3. Click to highlight the target PSK.

__ 4. Click **Delete**. A **Confirmation** box displays asking if you want to delete the PSK.

__ 5. Click **OK**.

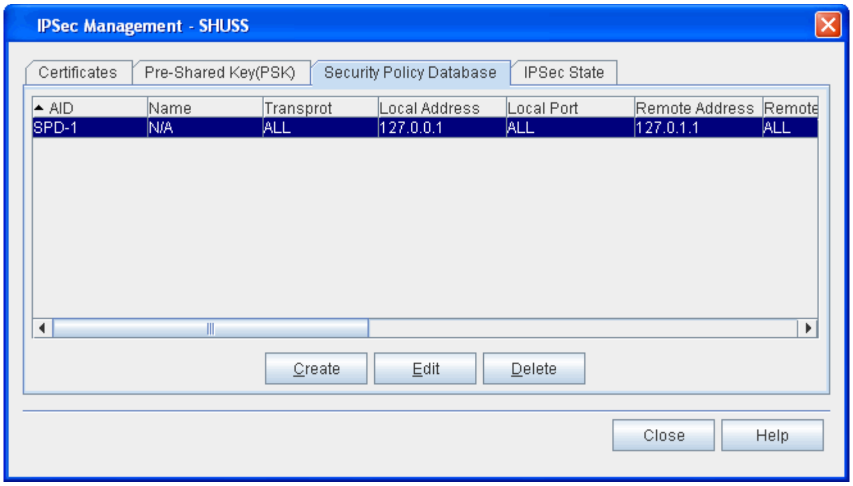
Provisioning Security Policy Databases

6.15 Provision security policy databases by performing the following steps:

__ 1. In the **Navigation Window**, right-click the NE icon to view the shortcut menu, then click **IPSec Management**. The **IPSec Management** dialog box displays.

__ 2. Click the **Security Policy Database** tab. Refer to Figure 6.25, page 15-68.

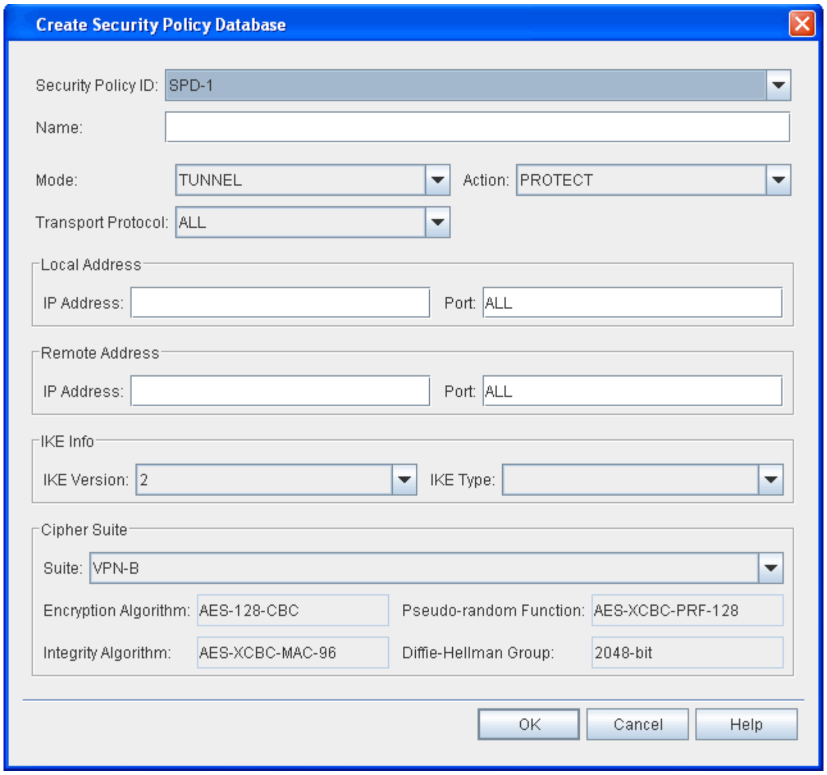
Figure 6.25 IP Sec Management, Security Policy Database Tab



AID	Name	Transprot	Local Address	Local Port	Remote Address	Remote
SPD-1	N/A	ALL	127.0.0.1	ALL	127.0.1.1	ALL

__ 3. Click **Create**. The **Create Security Policy Database** dialog box displays. Refer to Figure 6.26, page 15-68.

Figure 6.26 Create Security Policy Database



Security Policy ID: SPD-1

Name:

Mode: TUNNEL Action: PROTECT

Transport Protocol: ALL

Local Address

IP Address: Port: ALL

Remote Address

IP Address: Port: ALL

IKE Info

IKE Version: 2 IKE Type:

Cipher Suite

Suite: VPN-B

Encryption Algorithm: AES-128-CBC Pseudo-random Function: AES-XCBC-PRF-128

Integrity Algorithm: AES-XCBC-MAC-96 Diffie-Hellman Group: 2048-bit

__ 4. Click the **Security Policy ID** drop-down box to select the security policy identifier (**SPD-1–SPD-1000**).

__ 5. (Optional) Type a name for the security policy in the **Name** box (0–47 character string).

__ 6. Click the **Mode** drop-down box to specify the mode for the security policy (**TRANSPORT** or **TUNNEL**, default is **TUNNEL**).

__ 7. Click the **Action** drop-down box to select the security action taken for the policy: **PROTECT** if traffic is IPsec protected, **DISCARD** if traffic is not allowed to traverse the IPsec boundary, or **BYPASS** if traffic is allowed to traverse without IPsec protection.

__ 8. Click the **Transport Protocol** drop-down box to specify the transport protocol. The protocol number identifies the type of transport protocol used, as defined by the Internet Assigned Number Authority (IANA). (**1** for ICMP, **6** for TCP, **17** for UDP, **58** for ICMPv6, or **ALL** (default)).

__ 9. Complete the following information in the **Local Address** and **Remote Address** area:

__ 9.1 In the **IP Address** box, type the address or range of addresses where secured traffic will begin and the security policy will implement (local address) and where secured traffic will end and the security policy will stop (remote address). The format for the IP address is a double quoted string representing the IPv4 or IPv6 address.

- IPv4 address = "www.xxx.yyy.zzz"

Where:
w, **x**, **y**, **z** = **0**–**9**
www, **xxx**, **yyy**, **zzz** = **0**-**255**
The following IPv4 addresses are not allowed:
"224-255.xxx.xxx.xxx"
"169.254.xxx.xxx"
"127.xxx.xxx.xxx"
"10.0.0–3.xxx"
"0–1.xxx.xxx.xxx"

- IPv6 address = "x:x:x:x:x:x:x:x"

Where:
x = **0000**-**FFFF** (1–4 hexadecimal digits). The zero compression format is also supported (a double colon "::" indicates one or more groups of 16 bits of zeros).
The following IPv6 addresses are not allowed:
"0:0:0:0:0:0:0:1"

- Specify CIDR notation using a back slash and number representing the number of prefix bits, for example "172.32.7.5/16."

__ 9.2 In the **Port** box, type the local port or range of local ports allowed (**0**–**65535**, **ALL** to match all accessible port fields, or **OPAQUE** to match only port fields that are not accessible). Specify two ports for a range by separating the port numbers with a hyphen ("-"), for example "PortNumber-PortNumber."

Note: *The port number is based on the transport protocol value. If the Transport Protocol is 6 or 17, the port parameter can be 0–65535, ALL or OPAQUE. If the Transport Protocol is 1, 58, or ALL, the port parameter can be ALL or OPAQUE.*

__ 10. Complete the following information in the **IKE Info** area:

__ 10.1 Click the **IKE Version** drop-down box to select the Internet Key Exchange version (**1** or **2**, default is 2).

__ 10.2 Click the **IKE Type** drop-down box to select the authorization type for each security policy (**CERT** or **PSK-1**–**PSK-1000**, default is CERT).

__ 11. In the **Cipher Suite** area, click the **Suite** drop-down box to select the cipher suite used for the security policy (**VPN-A**, **VPN-B**, **VPN-A-NULL**, or **VPN-B-NULL**, default is VPN-B.) If the NE is configured for Federal Information Processing Standards (FIPS) secure mode, you can only use the VPN-B cipher suite.

__ 12. Verify the following information: **Encryption Algorithm**, **Integrity Algorithm**, **Pseduo-random Function**, and **Diffie-Hellman Group**.

Note: *For more information about Cipher Suite Algorithms, refer to the ENT-SPD command in the TL1 Command Reference Manual. Click the Help menu in the Craft Station to access this document.*

__ 13. Click **OK**.

Editing a Security Policy

6.16 Edit a security policy by performing the following steps:

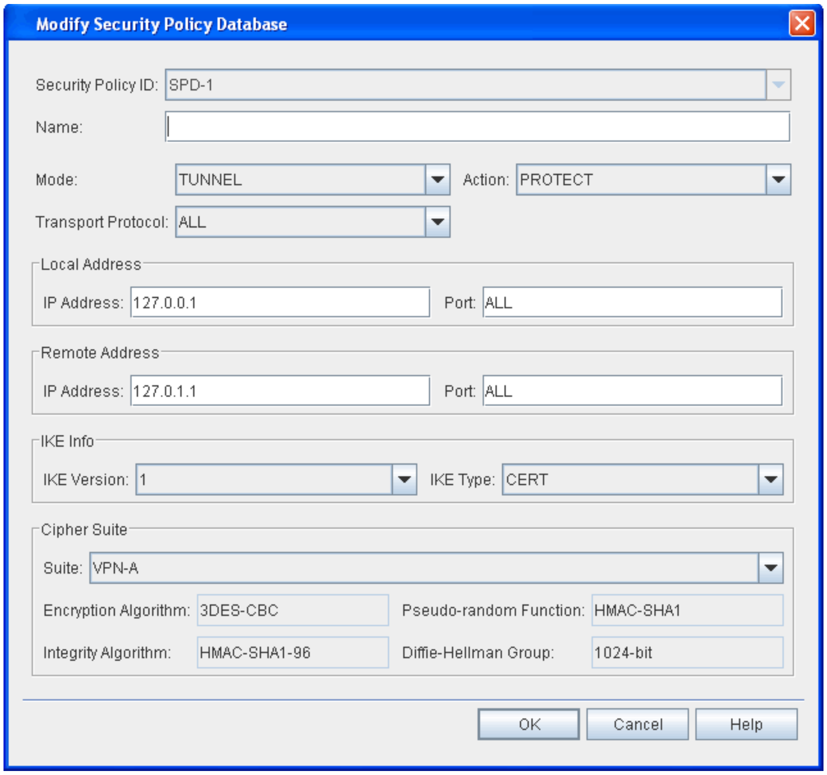
__ 1. In the **Navigation Window**, right-click the NE icon to view the shortcut menu, then click **IPSec Management**. The **IPSec Management** dialog box displays.

__ 2. Click the **Security Policy Database** tab.

__ 3. Click to highlight the target Security Policy Database.

__ 4. Click **Edit**. The **Modify Security Policy Database** dialog box displays. Refer to Figure 6.27, page 15-71.

Figure 6.27 Modify Security Policy Database



Modify Security Policy Database

Security Policy ID: SPD-1

Name:

Mode: TUNNEL Action: PROTECT

Transport Protocol: ALL

Local Address

IP Address: 127.0.0.1 Port: ALL

Remote Address

IP Address: 127.0.1.1 Port: ALL

IKE Info

IKE Version: 1 IKE Type: CERT

Cipher Suite

Suite: VPN-A

Encryption Algorithm: 3DES-CBC Pseudo-random Function: HMAC-SHA1

Integrity Algorithm: HMAC-SHA1-96 Diffie-Hellman Group: 1024-bit

__ 5. (Optional) Type a name for the security policy in the **Name** box (0–47 character string).

__ 6. Click the **Mode** drop-down box to specify the mode for the security policy (**TRANSPORT** or **TUNNEL**, default is **TUNNEL**).

__ 7. Click the **Action** drop-down box to select the security action taken for the policy: **PROTECT** if traffic is IPsec protected, **DISCARD** if traffic is not allowed to traverse the IPsec boundary, or **BYPASS** if traffic is allowed to traverse without IPsec protection.

__ 8. Click the **Transport Protocol** drop-down box to specify the transport protocol. The protocol number identifies the type of transport protocol used, as defined by the Internet Assigned Number Authority (IANA). (**1** for ICMP, **6** for TCP, **17** for UDP, **58** for ICMPv6, or **ALL** (default)).

__ 9. Complete the following information in the **Local Address** and **Remote Address** area:

__ 9.1 In the **IP Address** box, type the address or range of addresses where secured traffic will begin and the security policy will implement (local address) and where secured traffic will end and the security policy will stop (remote address). The format for the IP address is a double quoted string representing the IPv4 or IPv6 address.

- IPv4 address = "www.xxx.yyy.zzz"

Where:
w, **x**, **y**, **z** = **0**–**9**
www, **xxx**, **yyy**, **zzz** = **0**-**255**
The following IPv4 addresses are not allowed:
"224-255.xxx.xxx.xxx"
"169.254.xxx.xxx"
"127.xxx.xxx.xxx"
"10.0.0–3.xxx"
"0–1.xxx.xxx.xxx"

- IPv6 address = "x:x:x:x:x:x:x:x"

Where:
x = **0000**-**FFFF** (1–4 hexadecimal digits). The zero compression format is also supported (a double colon "::" indicates one or more groups of 16 bits of zeros).
The following IPv6 addresses are not allowed:
"0:0:0:0:0:0:0:1"

- Specify CIDR notation using a back slash and number representing the number of prefix bits, for example "172.32.7.5/16."

__ 9.2 In the **Port** box, type the local port or range of local ports allowed (**0**–**65535**, **ALL** to match all accessible port fields, or **OPAQUE** to match only port fields that are not accessible). Specify two ports for a range by separating the port numbers with a hyphen ("-"), for example "PortNumber-PortNumber."

Note: *The port number is based on the transport protocol value. If the Transport Protocol is 6 or 17, the port parameter can be 0–65535, ALL or OPAQUE. If the Transport Protocol is 1, 58, or ALL, the port parameter can be ALL or OPAQUE.*

__ 10. Complete the following information in the **IKE Info** area:

__ 10.1 Click the **IKE Version** drop-down box to select the Internet Key Exchange version (**1** or **2**, default is 1).

__ 10.2 Click the **IKE Type** drop-down box to select the authorization type for each security policy (**CERT** or **PSK-1**–**PSK-1000**, default is CERT).

__ 11. In the **Cipher Suite** area, click the **Suite** drop-down box to select the cipher suite used for the security policy (**VPN-A**, **VPN-B**, **VPN-A-NULL**, or **VPN-B-NULL**, default is VPN-B.) If the NE is configured for Federal Information Processing Standards (FIPS) secure mode, you can only use the VPN-B cipher suite.

__ 12. Verify the following information: **Encryption Algorithm**, **Integrity Algorithm**, **Pseduo-random Function**, and **DiffieHellman Group**.

Note: *For more information about Cipher Suite Algorithms, refer to the ENT-SPD command in the TL1 Command Reference Manual. Click the Help menu in the Craft Station to access this document.*

__ 13. Click **OK**.

Deleting a Security Policy

6.17 Delete a security policy by performing the following steps:

__ 1. In the **Security Policy Database** tab of the **IP Sec Management** dialog box, click to highlight one of the security policies.

__ 2. Click **Delete**. A **Confirmation** box displays.

__ 3. Click **OK** or **Cancel**.

Enabling or Disabling IPSec

6.18 Enable or disable the IPSec feature by performing the following steps:

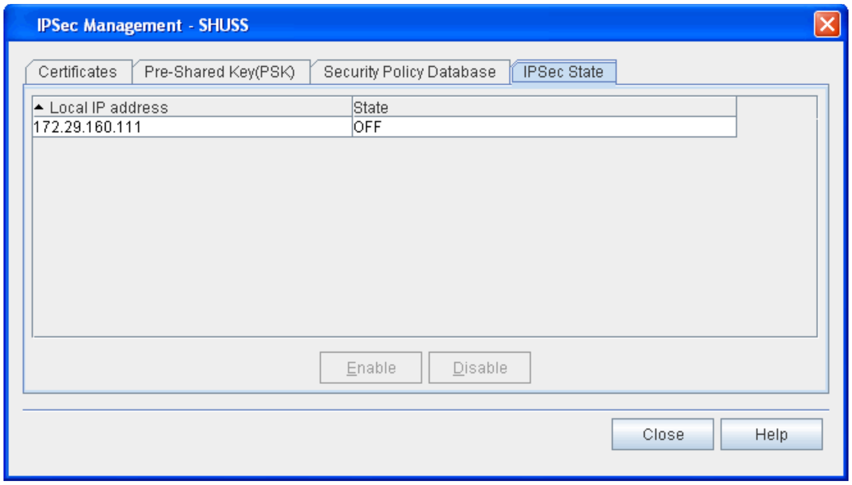
Note 1: *If you provision IP security incorrectly, communication may be lost with the NE when the IPSec feature is started. Confirm that all IP security settings are correct at the NE, the PC, and the Craft Station interface.*

Note 2: *If the Craft Station PC loses communication with the NE due to incorrect security settings after the IP Security feature is enabled, use the Inhibit IPSec feature to disable IP Security and then connect to the NE via the serial port until the security settings are resolved.*

__ 1. In the **Navigation Window**, right-click the NE icon to view the shortcut menu, then click **IPSec Management**. The **IPSec Management** dialog box displays.

__ 2. Click the **IPSec State** tab. Refer to Figure 6.28, page 15-74.

Figure 6.28 IPSec Management, IPSec State Tab



Local IP address	State
172.29.160.111	OFF

__ 3. You can configure the IPSec feature for each IP address. Verify the **Local IP address** and **State** in the table.

__ 4. IPSec defaults to OFF for each supported IP address. Change the state of the IPSec feature by performing the following steps:

__ 4.1 Click to highlight the target Local IP address.

__ 4.2 Click **Enable** or **Disable**. A **Confirmation** box displays.

__ 4.3 Click **OK** to continue or **Cancel** to stop the action. A **Message** box displays.

__ 4.4 Click **OK**.

__ 5. Click **Close**.

TCP/IP

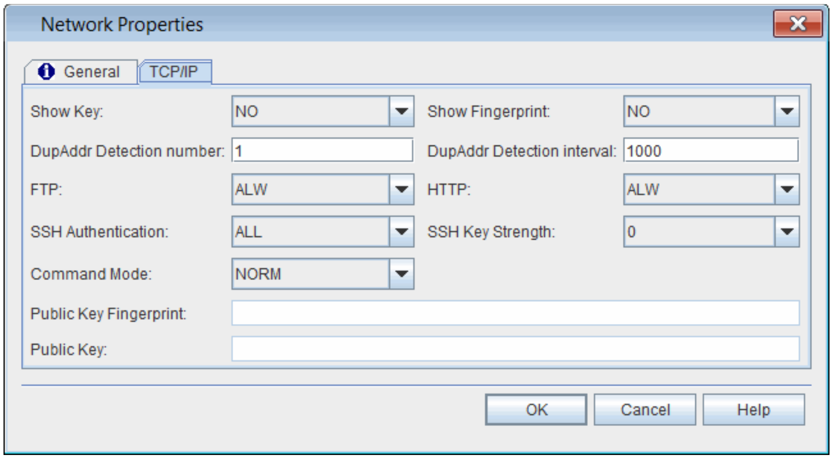
6.19 You can view and modify the attributes of a TCP/IP entity and secure communication service protocols such as SSH, sFTP and Tunneling of non-secure ports. The system defaults the authentication method to key-based and password-based.

6.20 View and modify TCP/IP attributes by performing the following steps:

__ 1. In the **Navigation Window**, right-click the NE to view the shortcut menu, then click **Network Properties**.

__ 2. Click the **TCP/IP** tab. Refer to Figure 6.29, page 15-75.

Figure 6.29 Network Properties - TCP/IP Tab



Show Key: NO
Show Fingerprint: NO
DupAddr Detection number: 1
DupAddr Detection interval: 1000
FTP: ALW
HTTP: ALW
SSH Authentication: ALL
SSH Key Strength: 0
Command Mode: NORM
Public Key Fingerprint:
Public Key:

__ 3. Click the **Show Key** drop-down box to specify whether or not to display the system public key string stored in the database (**YES** or **NO**).

__ 4. Click the **Show Fingerprint** drop-down box to specify whether or not to display the fingerprint of the system public key string stored in the database and the encoding scheme used to display the fingerprint. Select **HEX** to display the fingerprint encoded in hex. Select **BABBLE** to display the fingerprint encoded in Bubble Babble. Select **NO** if the system should not display the fingerprint.

__ 5. In the **DupAddr Detection** number box, type the number of neighbor solicitation messages sent when performing duplicate address detection on the interface. (**0**–**600**, setting the value to 0 disables this attribute).

__ 6. In the **DupAddr Detection** interval box, type the time interval for the NE to send neighbor solicitation messages when performing duplicate address detection (**1000** ms–**3600000** ms).

__ 7. Click the **FTP** drop-down box to specify whether FTP is allowed for both non-secure or secure mode, only secure mode, or if it should be inhibited. Select **ALW** to allow both non-secure and secure mode. Select **SECURE** to allow secure mode only. Select **INH** to inhibit FTP.

__ 8. Click the **HTTP** drop-down box to specify whether the HTTP server is allowed in both non-secure and secured mode (**ALW**) or inhibited (**INH**).

__ 9. Click the **SSH Authentication** drop-down box to specify the authentication method allowed for secure operations in SSH or sFTP. Select **KEY** to allow key-based authentication. Select **ALL** to allow key-based and password-based authentication.

__ 10. Click the **SSH Key Strength** drop-down box to specify the strength of the key for regenerating the private/public key pair in SSH or sFTP. Select **512** for key strength of 512, **1024** for key strength of 1024, **2048** for key strength of 2048, or **0** if no key strength is defined. The system default is 0. If you change this setting, the NE replaces the existing keys in the system with a newly generated private/public key pair of the specified key strength. If you do not change this setting, no change is made to the existing keys.

__ 11. Click the **Command Mode** drop-down box to select **NORM** (any inconsistencies prevent the system from executing changes) or **FRCD** (system executes changes regardless of inconsistencies).

__ 12. If the NE is configured to show the public key fingerprint used in SSH or sFTP, the fingerprint of the public key displays in the **Public Key Fingerprint** box (0 to 128 ASCII character string in double quotes).

__ 13. If the NE is configured to show the public key used in SSH or sFTP, the public key displays in the **Public Key** box. (The key may display in hex (x:x:x:x:x:x:x:x) where x represents a 2 digit hexadecimal number, or in babble (x-x-x-x-x-x-x-x-x-x-x) where x represents 5 alphanumeric characters.)

__ 14. Click **OK**.

Managing the Database

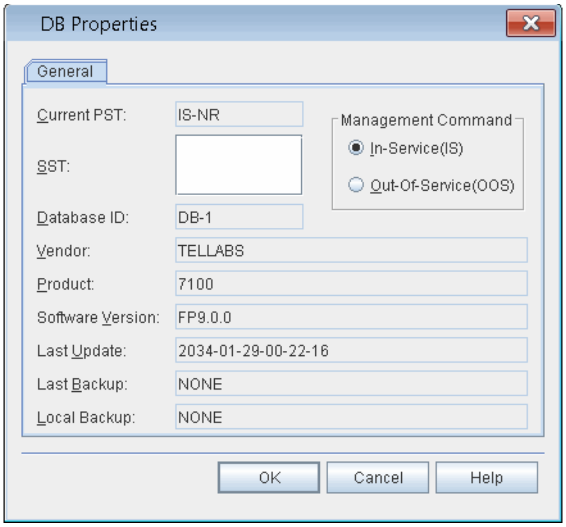
6.21 This section describes how to back up and restore the system database and how to schedule these activities.

Viewing the Database Properties

6.22 Review the properties of the database by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **DB-1 (Database)** icon to view the shortcut menu, then click **Properties**. The **DB Properties** dialog box displays. Refer to Figure 6.30, page 15-76.

Figure 6.30 DB Properties



Current PST: IS-NR

SST:

Database ID: DB-1

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

Vendor: TELLABS

Product: 7100

Software Version: FP9.0.0

Last Update: 2034-01-29-00-22-16

Last Backup: NONE

Local Backup: NONE

Most of the fields in this dialog box are read-only. Table 6.1, page 15-77 details each field and its definition. The **Management Command** parameter supports the **In-Service (IS)** or **Out-Of-Service (OOS)** or states.

__ 2. Click **OK** to save changes and close this screen. Click **Cancel** to close this screen without saving changes.

Table 6.1 Fields in Database Properties Dialog Box

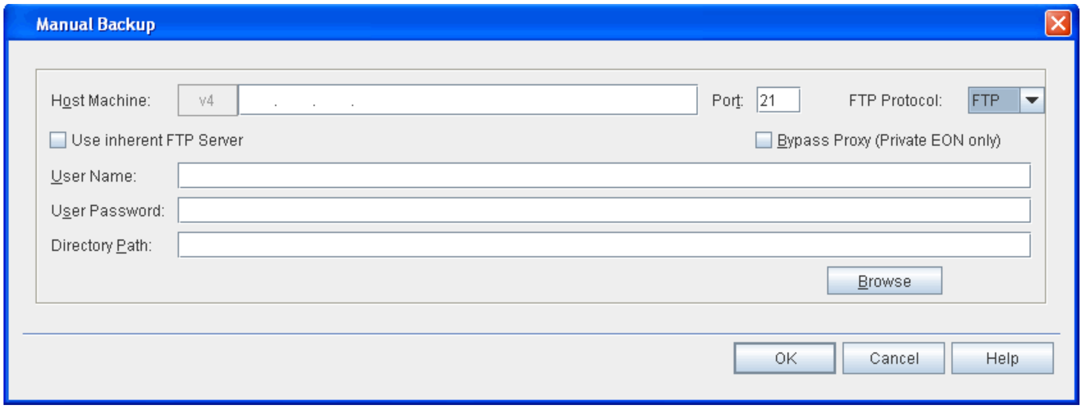
Field	Definition
Current PST	Current State of Database **IS**: In-Service **OOS**: Out-of-Service
SST	Secondary state of database
Database ID	Identifier for database (This is the icon label in the Navigation Window.)
Vendor	Manufacturer
Product	Product name
Software Version	Version of software in use
Last Update	Time and date of last software update
Last Backup	Time and date of last database backup
Local Backup	Identifies whether a local backup is present based on the last backup (using COPY-RFILE or SCHED-BACKUP-MEM) with the value: <yyyy-mm-dd>-<hh-mm-ss> (date of the local database backup) NONE if no local database backup exists
Management Command	Click In-Service(IS) or Out-Of-Service(OOS) to set the service state

Backing Up the Database

6.23 Back up the database by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **DB-1 (Database)** icon to view the shortcut menu. Point to **Manage Database**, then click **Backup**. The **Manual Backup** dialog box displays. Refer to Figure 6.31, page 15-77.

Figure 6.31 Manual Backup Screen



Host Machine: v4 . . .

Port: 21

FTP Protocol: FTP

□ Use inherent FTP Server

□ Bypass Proxy (Private EON only)

__ 2. Type the IP Address of the host machine where to store the backup files in the **Host Machine** box. (The format of the IP address–IPv4 or IPv6, is configured during basic commissioning.)

__ 3. Type the port number of the host machine in the **Port** box.

__ 4. Click the **FTP Protocol** drop-down box to select **FTP** (file transfer protocol) or **SFTP** (secure file transfer protocol).

__ 5. The Craft Station provides an inherent **FTP** server for file transfers to the NE. An FTP server may also be running on the PC (refer to Setting Up FTP, page 15-12). If you use the Craft Station FTP server to back up the database, click the **Use inherent FTP Server**.

__ 6. Leave the **Bypass Proxy (Private EON only)** box unchecked.

__ 7. Type the FTP server user name in the **User Name** box. This field automatically populates if you select the inherent FTP server.

__ 8. Type the FTP user password in the **User Password** box. This field automatically populates if you select the inherent FTP server.

__ 9. Use the **Browse** button to select the file path, or type the file path, where the files will be stored in the **Directory Path** box.

Note: *If the Craft Station does not have IP connectivity to the FTP server, you must type the file path manually instead of using the browse button.*

__ 10. Click **OK**.

__ 11. An **Information** box displays indicating the backup has begun. Click **OK**.

__ 12. Verify the database backup completes by monitoring the DB-1 (Database) icon in the Navigation Window. Progress increments from 0% to 100% with the final state indicating the last backup date and time is the current date and time.

Restoring the Database Backup

6.24 Restore the database by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **DB-1 (Database)** icon to view the shortcut menu, then click **Properties**. The **DB Properties** window displays.

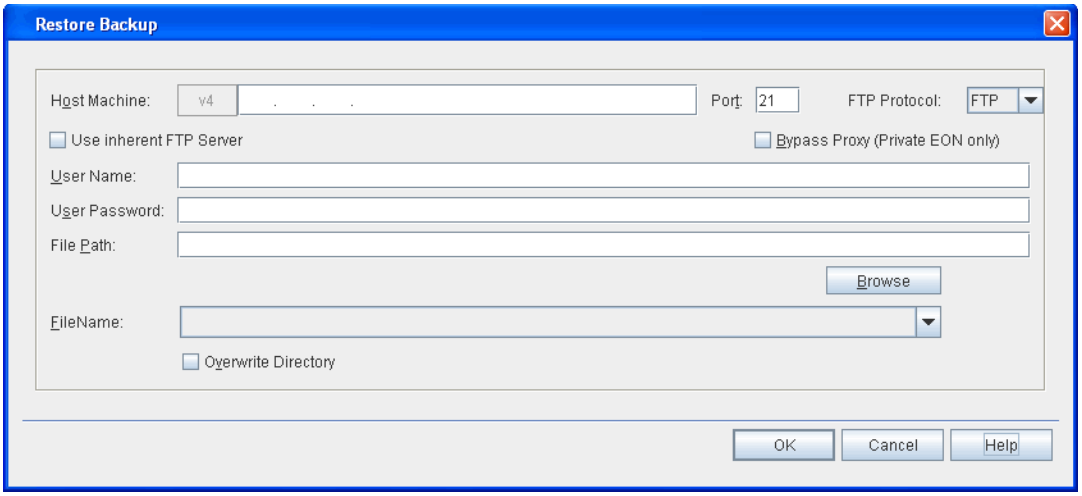
__ 2. In the **Management Command** area, confirm the state is **Out-Of-Service (OOS)**.

__ 2.1 If necessary, click **Out-Of-Service (OOS)** to set the database out-of-service.

__ 3. Click **OK**.

__ 4. In the **Navigation Window**, right-click the **DB-1 (Database)** icon to view the shortcut menu, point to **Manage Database**, then click **Restore.** The **Restore Backup** dialog box displays. Refer to Figure 6.32, page 15-79.

Figure 6.32 Database Restore Backup Screen



Restore Backup

Host Machine: v4 . . .   Port: 21   FTP Protocol: FTP

□ Use inherent FTP Server   □ Bypass Proxy (Private EON only)

User Name:

User Password:

File Path:

Browse

FileName:

□ Overwrite Directory

OK   Cancel   Help

__ 5. Type the IP Address of the host machine in the **Host Machine** box. (The format of the IP address–IPv4 or IPv6, is configured during basic commissioning.)

__ 6. Type the port number in the **Port** box.

__ 7. Click the **FTP Protocol** drop-down box to select **FTP** (file transfer protocol) or **SFTP** (secure file transfer protocol).

__ 8. The Craft Station provides an inherent **FTP** server for file transfers to the NE. An FTP server may also be running on the PC (refer to Setting Up FTP, page 15-12). If you intend to use the Craft Station FTP server to restore the database, click **Use inherent FTP Server**.

__ 9. Leave the **Bypass Proxy (Private EON only)** box unchecked.

__ 10. Type the FTP server user name in the **User Name** box. This field automatically populates if you select the inherent FTP server.

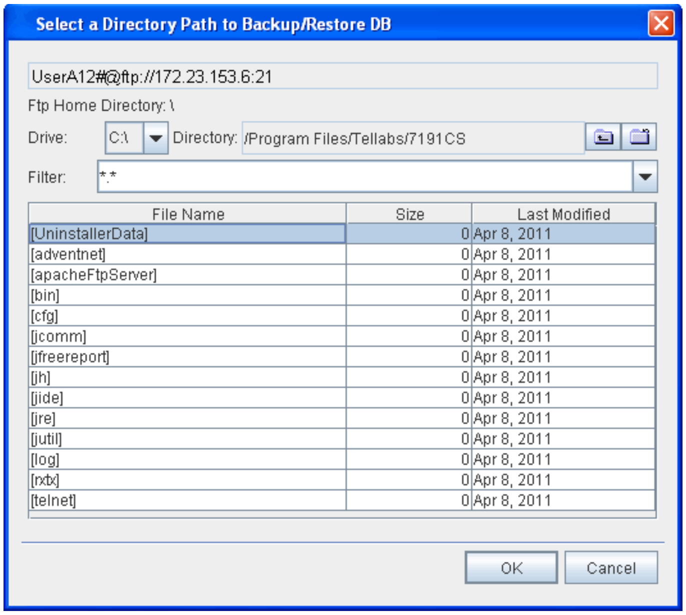
__ 11. Type the FTP server user password in the **User Password** box. This field is automatically populates if you select the inherent FTP server.

__ 12. Use the **Browse** button to select the file path, or type the file path of the saved database in the **Directory Path** box. If you clicked the **Use Inherent FTP Server** box in step 8, page 15-79 refer to Figure 6.33, page 15-80. Otherwise, refer to Figure 6.34, page 15-80.

If you use the **Browse** button, a selection of current folders displays. In this window, use the **Up** and **New** buttons to navigate or add directories. When you select the database folder, click **OK** and the window closes. The **Restore Backup** dialog box displays with the selected directory.

Note: *If the Craft Station does not have IP connectivity to the FTP server, you must type the file path manually instead of using the browse button.*

Figure 6.33 Select Directory Path for Database Backup (Using Inherent FTP Server)



UserA12#@ftp://172.23.153.6:21

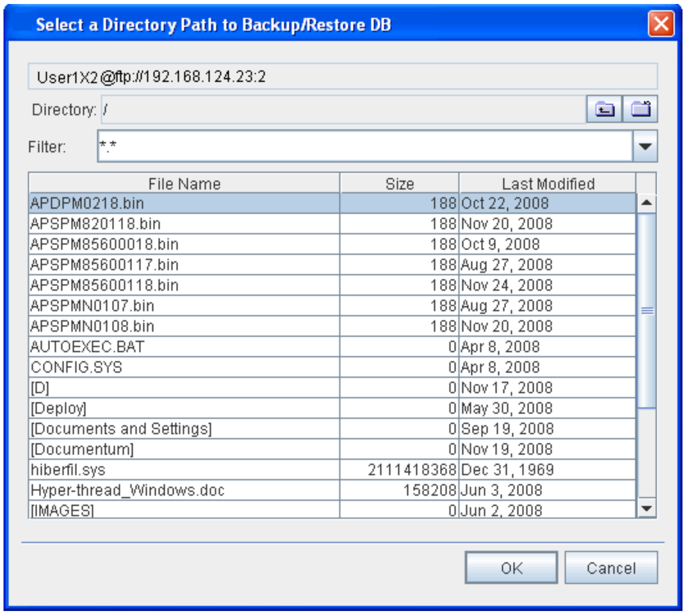
Ftp Home Directory: \

Drive: C:\ Directory: /Program Files/Tellabs/7191CS

Filter: *.*

File Name	Size	Last Modified
[UninstallerData]	0	Apr 8, 2011
[adventnet]	0	Apr 8, 2011
[apacheFtpServer]	0	Apr 8, 2011
[bin]	0	Apr 8, 2011
[cfg]	0	Apr 8, 2011
[jcomm]	0	Apr 8, 2011
[jfreereport]	0	Apr 8, 2011
[jh]	0	Apr 8, 2011
[jide]	0	Apr 8, 2011
[jre]	0	Apr 8, 2011
[jutil]	0	Apr 8, 2011
[log]	0	Apr 8, 2011
[rxtx]	0	Apr 8, 2011
[telnet]	0	Apr 8, 2011

Figure 6.34 Select Directory Path for Database Backup



User1X2@ftp://192.168.124.23:2

Directory: /

Filter: *.*

File Name	Size	Last Modified
APDPM0218.bin	188	Oct 22, 2008
APSPM820118.bin	188	Nov 20, 2008
APSPM85600018.bin	188	Oct 9, 2008
APSPM85600117.bin	188	Aug 27, 2008
APSPM85600118.bin	188	Nov 24, 2008
APSPMN0107.bin	188	Aug 27, 2008
APSPMN0108.bin	188	Nov 20, 2008
AUTOEXEC.BAT	0	Apr 8, 2008
CONFIG.SYS	0	Apr 8, 2008
[D]	0	Nov 17, 2008
[Deploy]	0	May 30, 2008
[Documents and Settings]	0	Sep 19, 2008
[Documentum]	0	Nov 19, 2008
hiberfil.sys	2111418368	Dec 31, 1969
Hyper-thread_Windows.doc	158208	Jun 3, 2008
[IMAGES]	0	Jun 2, 2008

__ 13. In the **Restore Backup** dialog box, click **Overwrite Directory** if the TID is different from the current NE TID. Refer to Figure 6.32, page 15-79.

__ 14. Click **OK**.

Note 1: *Prior to the NE reset, you can view the status of the restore process in the* ***Events*** *window of the Craft Station main screen.*

Note 2: *Restoring the database can take up to 30 minutes to complete and causes the NE to reset. Communication with the NE is lost during the reset.*

Restoring Local Database File

6.25 If a local database file exists on the NE, you can restore the local file of the NE database. The local database file is stored on the STPM and is a copy of the last successful user-initiated database backup.

6.26 Restore the local database file by performing the following steps:

__ 1. Verify that a local database file exists on the NE by performing the following steps:

__ 1.1 In the **Navigation Window**, right-click the **DB** icon to view the shortcut menu, then click **Properties**. The **Properties** dialog box displays.

__ 1.2 If a local database exists, the file name with the date of the local database backup (<yyyy-mm-dd>-<hh-mm-ss>) displays in the **Local Backup** box.

If a local backup exists, go to step 2, page 15-81. If a local backup does not exist, you cannot restore the local file of the NE database.

__ 2. Place the DB out-of-service by performing the following steps:

__ 2.1 In the **Management Command** area of the **DB Properties** dialog box, click **Out-of-Service (OOS)**. An **Information** box displays informing you that the database was placed out-of-service.

__ 2.2 Click **OK**.

__ 3. In the **Navigation Window**, right-click the **DB** icon to view the shortcut menu, point to **Manage Database**, then click **Local File Restore**. A Confirmation box displays asking if you want to do a local file restore.

__ 4. Click **OK**.

Note: *Restoring the database can take up to 30 minutes to complete and causes the NE to reset. Communication with the NE is lost during the reset.*

Restoring the Database Backup by Connecting to LCI Port (Empty Database Restoration)

6.27 Restoring the database by connecting to the local craft interface (LCI) port allows you to restore a lost or NULL database without affecting traffic. Restore the database by performing the following steps:

Note: *You need an administrator-level user name and password to perform this procedure. If you do not have the correct user name and password, follow your company's prescribed procedures for obtaining technical assistance, or contact the Coriant Technical Assistance Center at http://www.coriant.com/services_support.*

__ 1. Obtain a copy of the latest NE database backup file.

__ 2. Confirm the following information about the NE database backup file:

__ 2.1 Verify the database backup contains the ".CURRENT" extension and the most recent time stamp.

__ 2.2 Using the 7190/7194 management system, verify that the system identifier (name of the NE) matches the database backup file name that is targeted for database restoration.

The Craft Station will not be able to confirm the NE name. The NE may contain the default target identifier (TID) "Coriant" in place of the actual system identifier. The 7190/7194 management system will show the affected NE in the Navigation Window with a Red X next to it, indicating that the management system is unable to communicate with the NE.

__ 2.3 Verify that the name of the database backup file includes the system identifier of the target NE. For example, the database backup file named "SampleNetworkElement_FPxyz.CURRENT" corresponds to the NE named "SampleNetworkElement."

__ 3. Copy the database backup file directly to your laptop.

__ 4. Connect the laptop to the LCI port on the STPM. Refer to Commissioning an NE, page 15-11 for the procedure to connect a laptop to the LCI port.

__ 5. Launch the Craft Station software. Refer to Installing the Craft Station Software on a PC or Laptop, page 15-3 for installation instructions.

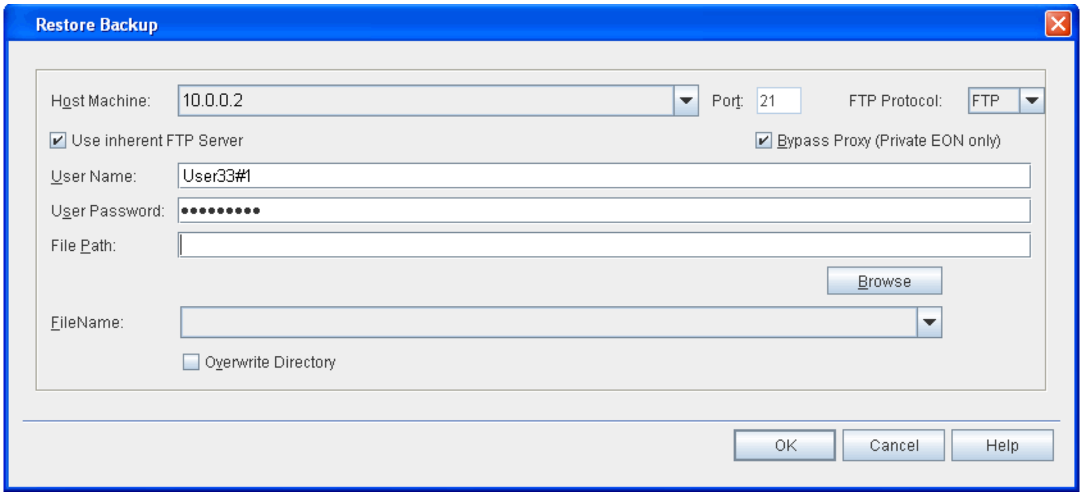
__ 6. In the **Navigation Window**, right-click the **DB-1 icon** to view the shortcut menu, then click **Properties**. The **DB Properties** window displays.

__ 7. Locate the **Current PST** box, and confirm it is set to **OOS**. If it is set to **IS-xx**, click **OOS** in the **Set Primary State (PST)** box.

__ 8. Click **OK**.

__ 9. In the **Navigation Window**, right-click the **DB-1** icon to view the shortcut menu, point to **Manage Database**, then click **Restore**. The **Restore Backup** dialog box displays. Refer to Figure 6.35, page 15-83.

Figure 6.35 Database Restore Backup Screen



Restore Backup

Host Machine: 10.0.0.2 Port: 21 FTP Protocol: FTP

☑ Use inherent FTP Server ☑ Bypass Proxy (Private EON only)

User Name: User33#1

User Password: •••••••••

File Path:

FileName:

☐ Overwrite Directory

__ 10. Click **Use Inherent FTP Server**. (The Craft Station provides an inherent **FTP** server for file transfers to the NE. An FTP server may also be running on the PC. Refer to Setting Up FTP, page 15-12.)

__ 11. Leave the **Bypass Proxy (Private EON only)** box unchecked.

Note: *The system automatically populates the **User Name** box and **User Password** box because you selected Use inherent FTP Server in step 10, page 15-83.*

__ 12. Select the IP Address of the host machine (where the NE Database is stored) from the **Host Machine** drop-down box.

__ 13. Type the port number in the **Port** box.

__ 14. Click the **FTP Protocol** drop-down box to select **FTP** (file transfer protocol) or **SFTP** (secure file transfer protocol).

__ 15. Use the **Browse** button to select the file path, or type the file path of the saved database in the **File Path** box.

If you use the **Browse** button, a selection of current folders displays. In this window, use the **Up** and **New** buttons to navigate or add directories. When you select the database folder, click **OK** and the window closes. The **Restore Backup** dialog box displays with the selected directory.

Note: *If the Craft Station does not have IP connectivity to the FTP server, you must type the file path manually instead of using the browser button.*

__ 16. In the **Restore Backup** dialog box, click **Overwrite Directory** if the TID is different from the current NE TID. Refer to Figure 6.35, page 15-83.

__ 17. Click **OK**.

Note 1: *Prior to the NE reset, you can view the status of the restore process in the **Events** window of the Craft Station main screen.*

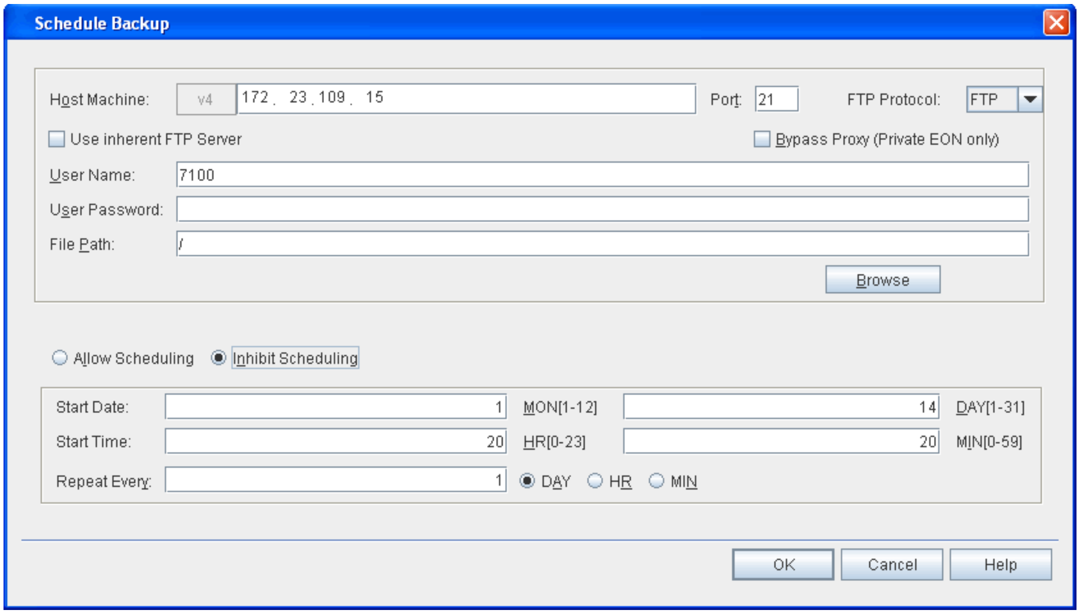
Note 2: *Restoring the database can take up to 30 minutes to complete and causes the NE to reset. Communication with the NE is lost during the reset.*

Scheduling Database Backups

6.28 Schedule database backups by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **DB-1** icon to view the shortcut menu, point to **Manage Database**, then click **Schedule**. The **Schedule Backup** window displays. Refer to Figure 6.36, page 15-84.

Figure 6.36 Schedule Backup



Schedule Backup

Host Machine: v4 172 . 23 . 109 . 15 Port: 21 FTP Protocol: FTP

□ Use inherent FTP Server □ Bypass Proxy (Private EON only)

User Name: 7100

User Password:

File Path: /

○ Allow Scheduling ● Inhibit Scheduling

Start Date: 1 MON[1-12] 14 DAY[1-31]

Start Time: 20 HR[0-23] 20 MIN[0-59]

Repeat Every: 1 ● DAY ○ HR ○ MIN

__ 2. Type the IP Address of the host machine where the backup files will be stored in the **Host Machine** box. (The format of the IP address–IPv4 or IPv6, is configured during basic commissioning.)

__ 3. Type the port number in the **Port** box.

__ 4. Click the **FTP Protocol** drop-down box to select **FTP** (file transfer protocol) or **SFTP** (secure file transfer protocol).

__ 5. The Craft Station provides an inherent **FTP** server for file transfers to the NE. An FTP server may also be running on the PC (refer to Setting Up FTP, page 15-12). If you intend to use the Craft Station FTP server to restore the database, click **Use Inherent FTP Server**.

__ 6. Leave the **Bypass Proxy (Private EON only)** box unchecked.

__ 7. Type the FTP server user name in the **User Name** box.

__ 8. Type the FTP server user password in the **User Password** box.

__ 9. Use the **Browse** button to select (or type) the path to where to store the backup files in the **File Path** box.

Note: *If the Craft Station does not have IP connectivity to the FTP server, you must type the file path manually instead of using the browse button.*

__ 10. To turn scheduling on, click **Allow Scheduling**. Or, Click **Inhibit Scheduling** to disable scheduled database backups.

__ 11. Type the date the backup should begin (**Start Date: Month, Day**).

__ 12. Type the time on that date the backup should begin (**Start Time: Hour, Minute**).

__ 13. Type the number of times the backup should repeat. Select the repeat interval by clicking the **DAY**, **HR**, or **MIN** option button.

__ 14. Click **OK**.

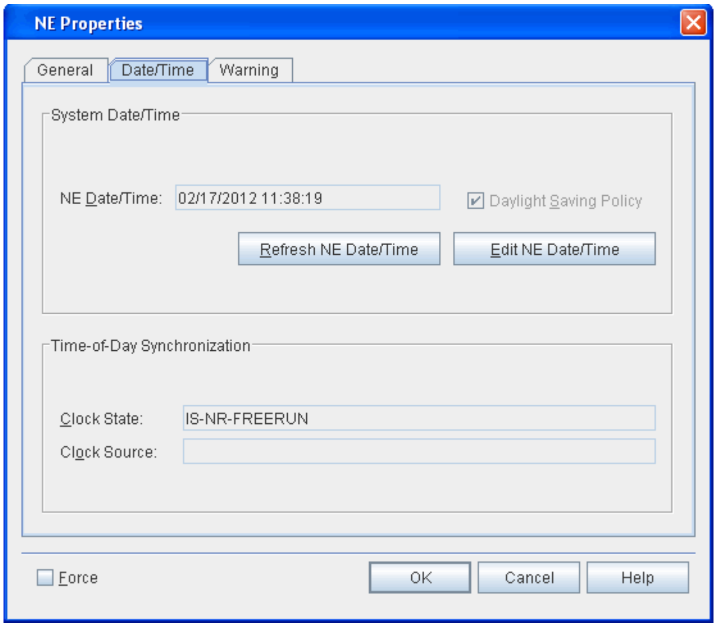
Managing Date and Time on the NE

6.29 This section describes how to access the dialog box used for provisioning the time and date parameters of the NE. Set the date and time in this dialog box if a network timing protocol (NTP) server is not providing timing.

__ 1. In the **Navigation Window**, right-click the **NE** icon to view the shortcut menu, then click **Properties**. The **NE Properties** dialog box displays.

__ 2. Click the **Date/Time** tab. The current date and time display. Refer to Figure 6.37, page 15-85.

Figure 6.37 Date/Time Tab in NE Properties



NE Properties

System Date/Time

NE Date/Time: 02/17/2012 11:38:19

☑ Daylight Saving Policy

Time-of-Day Synchronization

Clock State: IS-NR-FREERUN

Clock Source:

□ Force

__ 3. Click **Refresh NE Date/Time**. The Craft Station retrieves the current date and time from the NE and displays the updated date and time.

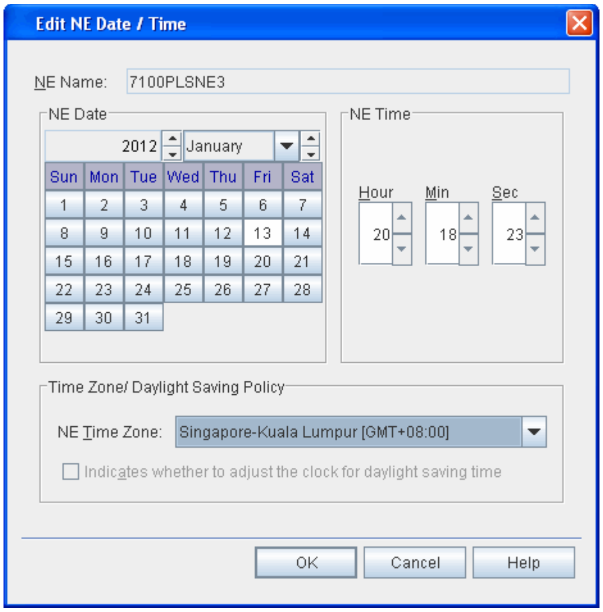
__ 4. In the **Time-of-Day Synchronization** area, the **Clock State** box shows the state of the timing source.

- __ **IS-NR-EXTERNAL** indicates the NE providing timing is receiving time and date information from an NTP device. (The date and time cannot be edited.)
- __ **IS-NR-FREERUN** indicates the NE providing timing is set to free run. Time and date are set manually at each NE.

The **Clock Source** box displays the IP address of the NTP server.

__ 5. Click **Edit NE Date/Time** to change the date, time, or daylight saving policy settings. Click **OK**. Refer to Figure 6.38, page 15-86.

Figure 6.38 Edit NE Date and Time



Edit NE Date / Time

NE Name: 7100PLSNE3

NE Date

2012 January

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

NE Time

Hour: 20 Min: 18 Sec: 23

Time Zone/ Daylight Saving Policy

NE Time Zone: Singapore-Kuala Lumpur [GMT+08:00]

☐ Indicates whether to adjust the clock for daylight saving time

NTP Peer Configuration

6.30 Each NE can receive date and time settings from a central Network Timing Protocol (NTP) server, eliminating the requirement to provision the date and time manually. Configure a maximum of two NTP Peers per NE. Provision the IP address of the NTP server at a gateway network element (GNE). The GNE then provides the NTP reference for its associated remote network elements (RNEs).

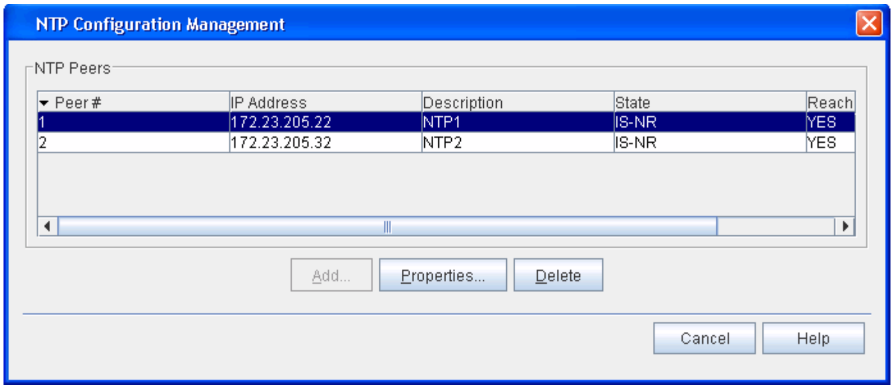
6.31 When the mTera NE is participating in the Private EON, the user shall provision the PGNEs as the NTPPEERs of the mTera.

6.32 Configure Network Timing Protocol (NTP) by performing the following steps:

__ 1. Contact your system administrator for the Data Communications Network (DCN) information required to access an NTP Server, including the IP address for the NTP Server.

__ 2. In the **Navigation Window**, right-click the **NE** icon (of the NE that is the PGNE) to view the shortcut menu, then click **NTP Peer Configuration**. Refer to Figure 6.39, page 15-87.

Figure 6.39 NTP Peer Configuration

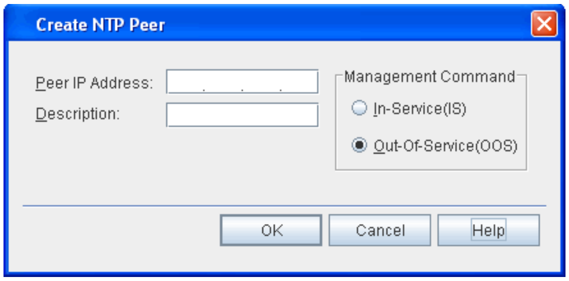


Peer #	IP Address	Description	State	Reach
1	172.23.205.22	NTP1	IS-NR	YES
2	172.23.205.32	NTP2	IS-NR	YES

__ 3. Add NTP peers by performing the following steps:

__ 3.1 Click the **Add** button, and the **Create NTP Peer** dialog box displays. Refer to Figure 6.40, page 15-87.

Figure 6.40 Create NTP Peer



Peer IP Address: . . .

Description:

Management Command

○ In-Service(IS)

● Out-Of-Service(OOS)

__ 3.2 Type the **IP** address (Peer IP) and a description of the peer that should also reference the NTP server.

__ 3.3 In the **Management Command** area, click **IS (In-Service)** for the NE to begin referencing the server.

__ 3.4 Click **OK**.

__ 4. To review the properties of NTP peers, highlight any of the Peers in the list and click **Properties** in the dialog box.

__ 5. Delete an NTP peer by performing the following steps:

__ 5.1 Highlight the NTP Peer in the list.

__ 5.2 Click the box in the **State** column and set the NTP Peer out-of-service.

__ 5.3 Highlight the same NTP Peer again, and click **Delete**.

Note: *The Craft Station only allows you to delete GNE peers. You cannot delete RNE peers.*

__ 5.4 Click **OK**.

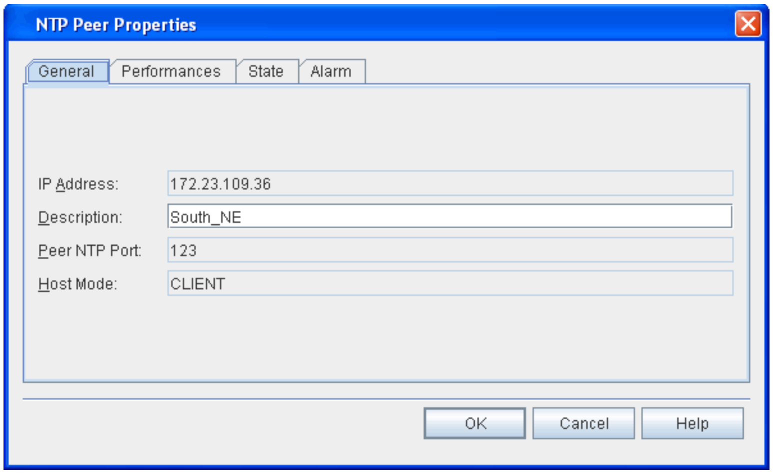
NTP Peer Properties

6.33 At the **NTP Peer Configuration** dialog box, you can highlight any of the NTP Peers in the list, and click the **Properties** button to review the NTP settings of that NE.

6.34 The dialog box opens to the **General** tab, where you can review the following information. Refer to Figure 6.41, page 15-88.

- **IP Address**: IP address of the NTP Peer.
- **Description**: Optionally add a description of the NTP Peer.
- **Peer NTP Port**: Port number to transfer NTP packets on the host. Use port **123** unless otherwise directed.
- **Host Mode**: This value is set to **CLIENT**, describing the NE relationship to the NTP host.

Figure 6.41 NTP Properties - General Tab



IP Address: 172.23.109.36

Description: South_NE

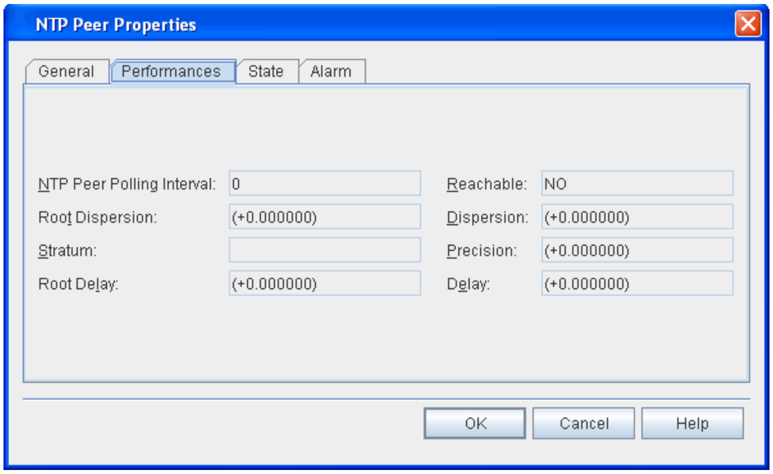
Peer NTP Port: 123

Host Mode: CLIENT

6.35 Click the **Performances** tab to review the following NTP Peer information: **NTP Polling Interval**, **Root Dispersion**, **Stratum**, **Root Delay**, if Peer is **Reachable**, **Dispersion**, **Precision**, and **Delay**. Refer to Figure 6.42, page 15-89.

Note: *Refer to TL1 Command Reference Manual for detailed description of these fields. Click the Help menu in the Craft Station to access this document.*

Figure 6.42 NTP Properties - Performances Tab



NTP Peer Polling Interval: 0

Reachable: NO

Root Dispersion: (+0.000000)

Dispersion: (+0.000000)

Stratum:

Precision: (+0.000000)

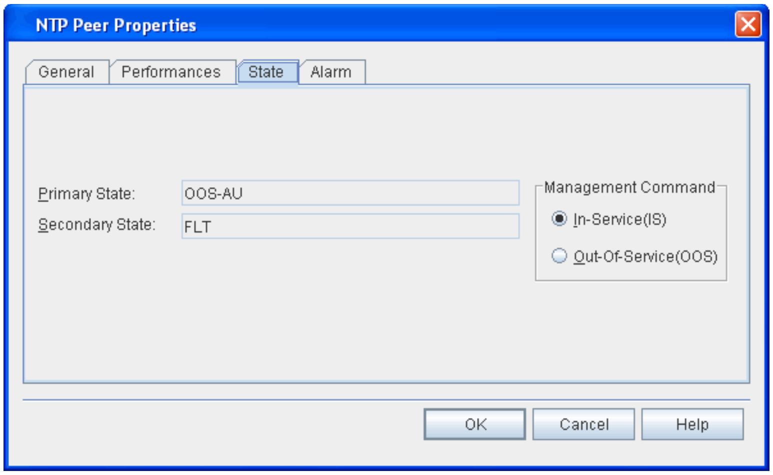
Root Delay: (+0.000000)

Delay: (+0.000000)

6.36 Click the **State** tab to review the current **Primary** and **Secondary State** of the NTP Peer and modify the **Present State** to In Service or Out of Service. Refer to Figure 6.43, page 15-89.

Note: *Refer to TL1 Command Reference Manual for additional details on system settings. Click the Help menu in the Craft Station to access this document.*

Figure 6.43 NTP Properties - State Tab



Primary State: OOS-AU

Secondary State: FLT

Management Command

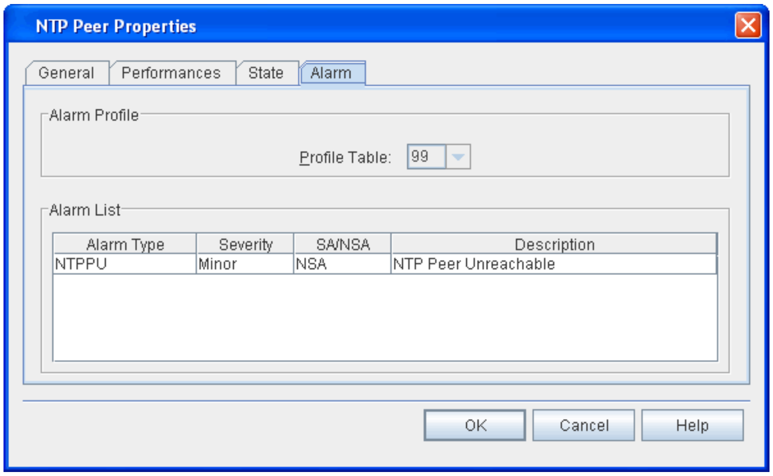
● In-Service(IS)

○ Out-Of-Service(OOS)

6.37 Click the **Alarm** tab to review the **Alarm Type**, **Severity**, **SA/NSA** status, and **Description** of current alarms on the NTP Peer. The **Alarm Profile** parameter defaults to 99. Refer to Figure 6.44, page 15-90.

Note: *Refer to TL1 Command Reference Manual for detailed definitions of alarm codes. Click the Help menu in the Craft Station to access this document.*

Figure 6.44 NTP Properties - Alarm Tab



Profile Table: 99

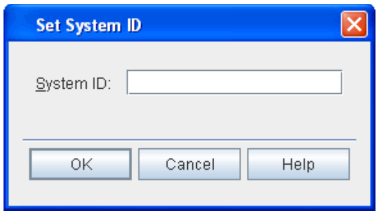
Alarm Type	Severity	SA/NSA	Description
NTPPU	Minor	NSA	NTP Peer Unreachable

Setting the System ID

6.38 Set the system ID by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NE icon** to view the shortcut menu, then click **Set System ID**. The **Set System ID** dialog box displays. Refer to Figure 6.45, page 15-90.

Figure 6.45 Set System ID



__ 2. Type an alphanumeric identifier for the system (maximum of 20 characters).

__ 3. Click **OK**.

Managing Router Interfaces

6.39 View router entries for Open Shortest Path First (OSPF) interfaces individually. The Craft Station retrieves and displays each interface on the router with descriptive fields for each. Refer to the ED-IF-ROUTER command in *TL1 Command Reference Manual* for additional details on router parameters. Click the Help menu in the Craft Station to access this document.

mTera EON

6.40 Configure the embedded operations network (EON) functionality of an mTera NE using proxy mode parameter. The proxy mode determines the mode of the applications running on the NE.

Client Proxy Mode

6.41 When the mTera NE participates in the legacy private EON and serves the networking function of private remote network element (PRNE), configure the proxy mode as "CLIENT." This means the applications mTera need the application gateways (which are running on the private gateway network element (PGNE)) to communicate with its application server.

Disabled Proxy Mode

6.42 When the mTera NE is directly connected to the customers DCN using the public IP address space, configure the proxy mode as "DISABLED." When the proxy mode of mTera is disabled all applications on the mTera connect directly to the application server or client without application gateways.

6.43 The 7100 OTS/7100 Nano NEs have three network partitions. NP-1 is the MCN partition, which carries the management traffic. NP-2 is the SCN partition, which carries the control plane signaling traffic. NP-3 is the TPCP (Transport Plane Control Plane) partition.

6.44 The mTera differs because it does not have a dedicated NP-2 SCN partition. The mTera supports both management traffic (TL1, SNMP) and Control Plane signaling traffic (RSVP) on the single network partition (NP-1). (NP-3 supports transport plane control plane traffic.)

6.45 When the mTera NE operates in a private EON environment, some of mTera Network interfaces can be configured in the Private EON MCN with the OSPFAREA 0.0.0.0 and some others can be configured in the SCN with the SCN's OSPF AREA. All the MCN interfaces and SCN interface on the mTera are in the single network partition (NP-1).

6.46 In the flat IP mode (mTera NE operates with the public IP addresses and directly connects to the customer's DCN) mTera EON also can configure its network interfaces into two different DCN and SCN OSPF areas to support management and signaling in the single network partition. A special case is the customer's DCN and SCN in the same OSPF network, in this case, the single network interface of mTera (for example, the DCN port) will carry both management and signaling traffic.

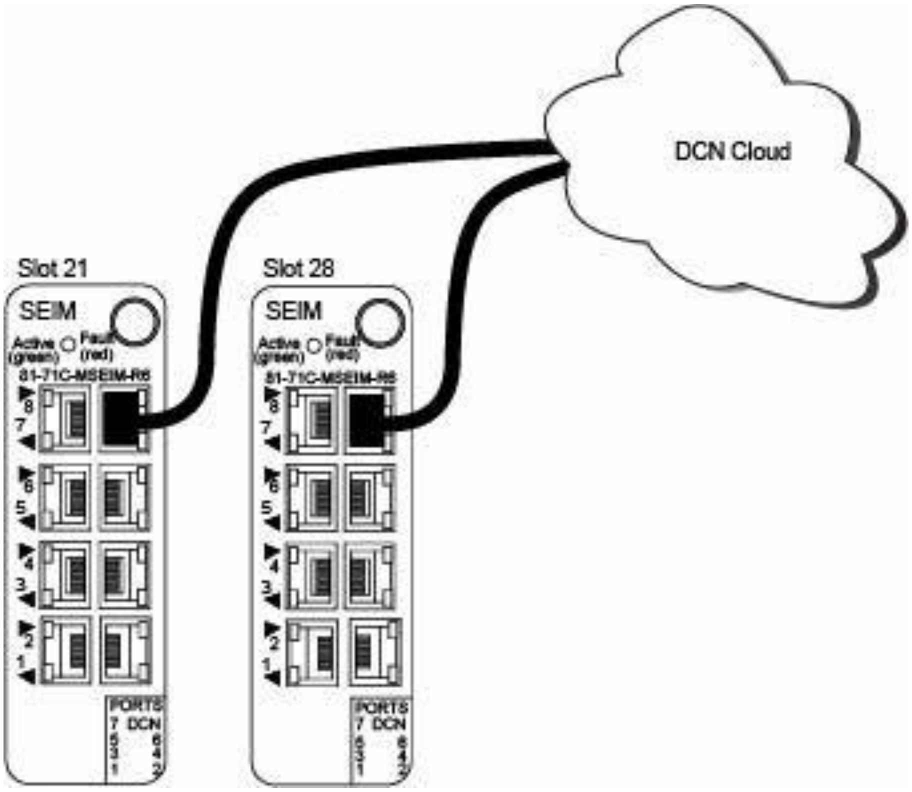
Interfaces on mTera EON

6.47 There are five kinds of interfaces on the mTera EON: SEIM Ethernet interfaces, LCI, GCC, IPPG (IP Protection Group) and SINTF-1(Stable Interface).

6.48 On one mTera NE there are up to two SEIM modules and each SEIM has eight Ethernet interfaces to be configured in the EON. One of the eight Ethernet interfaces is DCN interface and the others can be reconfigured. mTera EON also supports the GCC interfaces on the port modules.

6.49 Figure 6.46, page 15-92 shows the Ethernet cable connections between an mTera NE and the DCN. The connection is used for an mTera participating in a Private EON network. When the SEIM ETHERNET interfaces connect to other collocated NEs, the interface must be configured as point-to-point Ethernet ports ("unnumbered" via ENT-TL).

Figure 6.46 Cable mTera Shelf to 7100 Nano Shelf



6.50 In the mTera EON, the IP address of an interface is provisioned on the TL (topological link) entity and the TL is created on the physical or logical interfaces (with the exception of the LCI interface).

6.51 The MCN partition of 7100 OTS/7100 Nano NE is automatically configured. The NP, OSPF entity, OSPFAREA and NODE of MCN are implicitly created and cannot be modified. The TLs of DCN, SW, RT, MGMTIF are also implicitly created when ED-NET command is provisioned on the 7100 OTS/7100 Nano NE.

6.52 However, on the mTera NE, to make it more flexible and easy to control, the OSPF entity, OSFPAREA, NODE and all the TLs are explicitly created. There is no ED-NET command on the mTera NE. The TLs, including the TLs with SEIM ports as resources are created and edited by the standard ENT-TL and ED-TL commands.

Note: *For an mTera participating in the legacy Private EON, the OSPF controller RTRID of OSPF-1-1 must match one of the provisioned stable interface (SINTF-1) IP addresses in the OSPF area 0.0.0.0.*

Provisioning GCC

6.53 A GCC (General Communications Channel) interface is an in-band channel of an ODU or an OTU on the OSM-2C or OSM-2S. No special cabling is required.

6.54 GCC connectivity uses interfaces on the switching modules. GCC routes facility traffic to the appropriate network elements. Use GCC for management communication on links without an optical supervisory channel (OSC). All EON application protocols, such as FTP, TL1, SNMP and DHCP are supported through GCC links. DIR_OSC is not supported.

6.55 The mTera uses its Internal control ethernet network to carry facility interface embedded communications such as GCC to the shelf STPM. GCC Channels are supported in OTN interfaces. A facility can represent different layer functions in different port modules. The relations between facility and layer are listed below:

- OCH-P facility represents OCH+OTUk layers in OSM-2C and OSM-2S switching modules.
- OTUk facility represents OTUk layer in OSM-2C and OSM-2S switching modules.

Note: *The system supports IP/PPP over GCC. OSI over GCC is not supported.*

6.56 GCC using the OSM-2C supports:

- 45 GCC channels
- GCC0 is supported on the OTUk interface
- Control Plane signaling using IPv4 over GCC in Network Partition 1 on mTera standalone NE.
- HDLC bandwidth at least 136.6 Mbps, IP bandwidth at least 40 Mbps per OSM-2C

6.57 GCC using the OSM-2S supports:

- 60 GCC channels
- GCC0 is supported on the OTUk or OCH-P interface
- Control Plane signaling using IPv4 over GCC in Network Partition 1 on mTera standalone NE.

Note: HDLC bandwidth at least 78.75Mbps, IP bandwidth at least 40 Mbps per OSM-2S

6.58 A shelf supports 840 GCC channels. Data rates are as follows:

- peak data rate of 185 Mbps per shelf
- The mTera supports aggregate IP forwarding bandwidth up to 40 Mbps per OSM-2C and OSM-2S.

Requirements for General Communication Channel (GCC)

6.59 The GCC function requires the following items:

- Two OSM-2C and OSM-2S. These modules route facility traffic to the appropriate network elements.

6.60 The TL for a GCC node assigns the IP addresses and routing parameters to the resource (ODUk or OTUk) so that it can form an adjacency with the far end resource.

MCN Application

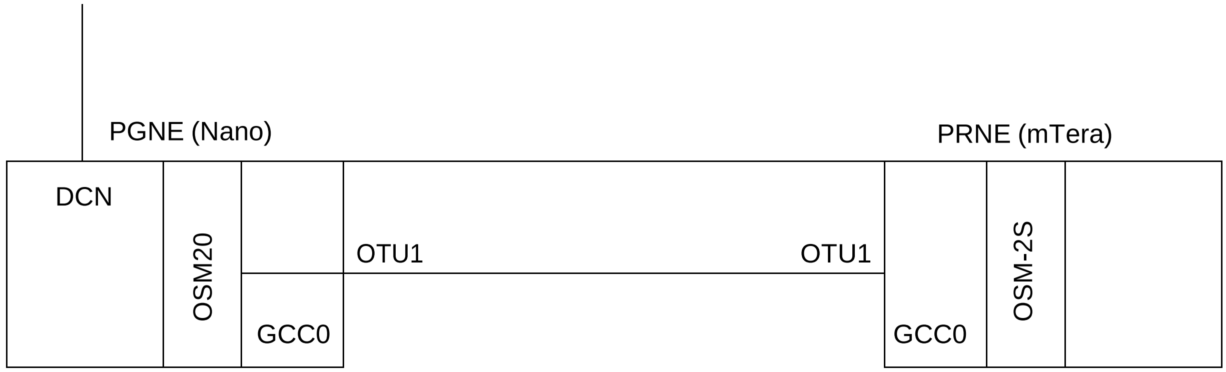
6.61 On the mTera NE, to make it more flexible and easy to control, the OSPF entity, OSFPAREA, NODE and all the TLs shall be explicitly created. The TLs, including the TLs with SEIM ports as resources are created and edited by the standard ENT-TL and ED-TL commands.

Note: *Refer to Control Plane, page 15-235 or TL1 Command Reference Manual for information about creating control plane entities.*

6.62 The following is an overview of the steps to create an MCN for GCC:

1. Create the OTN entity. Refer to Provisioning Facilities, page 15-188.
2. Create GCC on OTN entity. Refer to Creating GCC, page 15-95
3. Create a TL to link the GCC0 channel to the management IP. Refer to Figure 6.47, page 15-95.

Figure 6.47 MCN Application, TL Examples



```
ENT-TL::TL-1-1-51:ctag:::TLNAME="MCN TL for GCC",
NEADDRT=NUM,NEADDR=100.0.0.2,NDISCOVERY=
ENABLED,NEMASK=255.255.255.0,LINKPF=LINKPF-97,
ROUTING=ACTIVE,RAID=0.0.0.0,
RESOURCE=GCC0-9-15-1:IS;
```

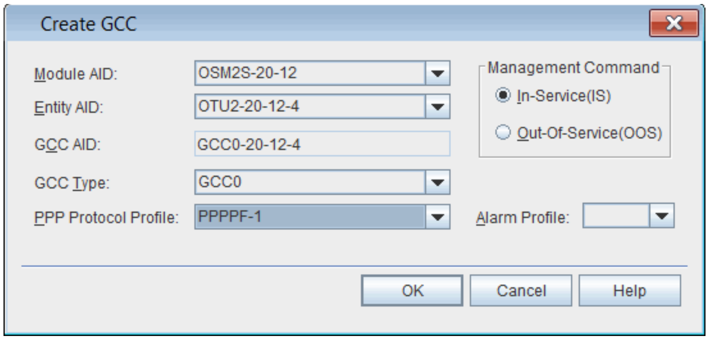
```
ENT-TL::TL-1-1-51:ctag:::TLNAME="MCN TL for GCC",
NEADDRT=NUM,NEADDR=100.0.0.2,NDISCOVERY=
ENABLED,NEMASK=255.255.255.0,LINKPF=LINKPF-97,
ROUTING=ACTIVE,RAID=0.0.0.0,
RESOURCE=GCC0-20-12-4:IS;
```

Creating GCC

6.63 Provision a GCC by performing the following steps:

__ 1. In the **Navigation Window**, right-click the facility or **GCC** icon to view the shortcut menu, then click **Create GCC Channel**. The **Create GCC** dialog box displays. Refer to Figure 6.48, page 15-95.

Figure 6.48 Create GCC


Create GCC

Module AID: OSM2S-20-12
Entity AID: OTU2-20-12-4
GCC AID: GCC0-20-12-4
GCC Type: GCC0
PPP Protocol Profile: PPPPF-1

Management Command
● In-Service(IS)
○ Out-Of-Service(OOS)

Alarm Profile:

__ 2. Click the **Module AID** drop-down box to select the module supporting the GCC entity.

__ 3. Click the **Entity AID** drop-down box to select the facility supporting the GCC entity.

__ 4. Click the **GCC Type** drop-down box to specify the GCC type:

- GCC0 - GCC channel using OTUk GCC0 bytes

__ 5. Click the **PPP Protocol Profile** to select the AID of the PPP entity.

__ 6. Click the **Alarm Profile** drop-down box to select an alarm profile (**0**–**20**, **99**). The default is 99.

__ 7. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

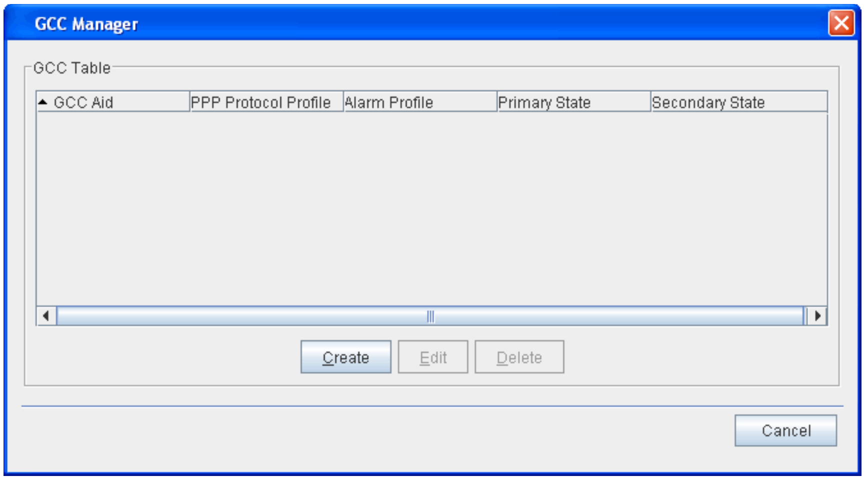
__ 8. Click **OK**.

Managing GCC

6.64 Perform the following steps to view or modify a GCC:

__ 1. In the **Navigation Window**, right-click the **GCC** icon to view the shortcut menu, then click **GCC Management**. The **GCC Manager** dialog box displays. Refer to Figure 6.49, page 15-96.

Figure 6.49 GCC Manager



GCC Aid	PPP Protocol Profile	Alarm Profile	Primary State	Secondary State

__ 2. View the following information in the GCC Table:

- GCC AID
- PPP Protocol Profile
- Alarm Profile
- Primary State
- Secondary State

__ 3. (Optional) Click Create to provision a new GCC.

__ 4. (Optional) To modify the properties of a GCC, click to highlight the GCC and click Edit.

__ 5. (Optional) To delete a GCC, click to highlight the GCC and click Delete.

Upgrading the NE Software

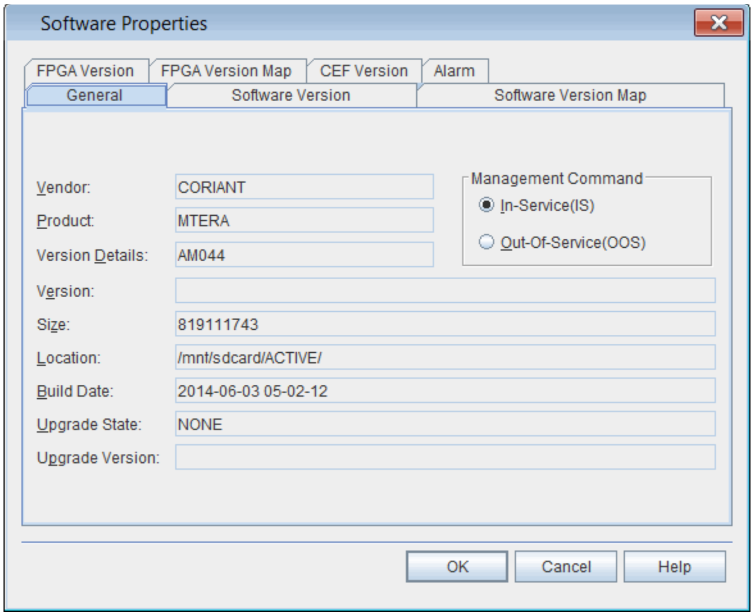
6.65 This section describes how to access the upgrade features on the Craft Station. For a complete description of how to upgrade an NE, refer to *FP1.0.x NE Upgrade Procedure.*

Viewing NE Software Properties

6.66 View the properties of the NE software by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **SW-1 - Software** icon to view the shortcut menu, then click **Properties**. The **Software Properties** dialog box displays. Refer to Figure 6.50, page 15-97.

Figure 6.50 Software Properties



Vendor: CORIANT
Product: MTERA
Version Details: AM044
Version:
Size: 819111743
Location: /mnt/sdcard/ACTIVE/
Build Date: 2014-06-03 05-02-12
Upgrade State: NONE
Upgrade Version:

Management Command
● In-Service(IS)
○ Out-Of-Service(OOS)

__ 2. Verify that the **General** tab is selected.

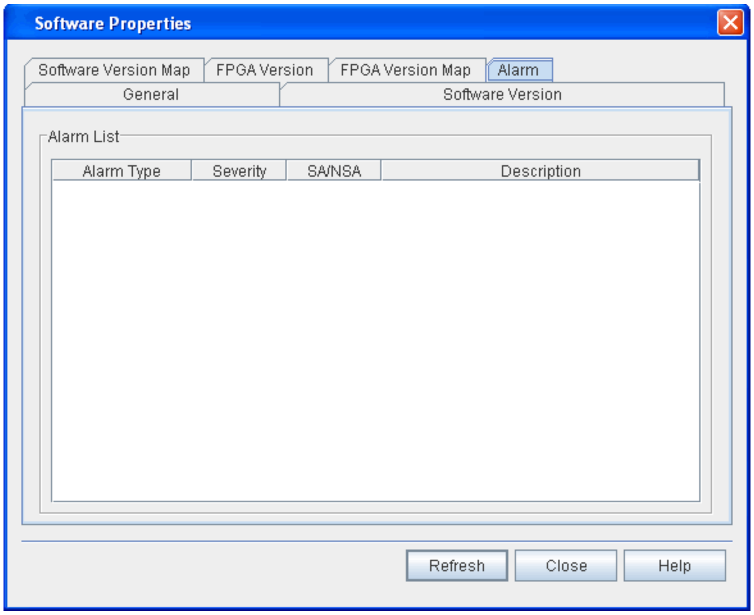
__ 3. Verify the following information:

- **Vendor**: CORIANT
- **Product**: product number
- **Version Details**: software identifier
- **Version**: feature package
- **Size**: space required
- **Location**: directory where located
- **Build Date**: date released
- **Upgrade State**: current state if in upgrade

- **Upgrade Version**: upgrade software identifier
- **Management Command**: state of software: In-Service (IS) or Out-Of-Service (OOS)

__ 4. Click the **Alarm** tab. Refer to Figure 6.51, page 15-98.

Figure 6.51 Software Properties, Alarm Tab



__ 5. Verify the following information in the **Alarm List** area:

- **Alarm Type**
- **Severity** (Critical, Major, Minor, Not Reported)
- **SA/NSA** (service affecting/non-service-affecting)
- **Description**

__ 6. Click **Close**.

NE Software Upgrade

6.67 For the procedure to upgrade NE software, refer to *NE Upgrade Procedure*.

Dynamic Software Configuration

6.68 The Dynamic Software Configuration (DSC) feature is applicable to a predefined set of software features and enables modification of released software by loading a new Capability Extension File (CEF) onto the NE defining the updated operational parameters.

6.69 Each NE feature package release contains software executables as well as a set of default CEFs. The NE software features supporting Dynamic Software Configuration always uses local default CEFs to set its behavior.

6.70 Dynamic configuration is enabled by substituting the default CEFs with one distributed by Coriant post-release of the NE software feature package.

6.71 The process model is similar to patching the NE; however no reset is required to adopt the updated software behavior. New CEFs may be applied outside of an upgrade or patch process by simply copying a new file to the NE. CEFs can copied manually to the NE as part of the software upgrade process to allow the manually specified CEF to supersede the CEF contained in the new software feature package.

Capability Extension File

6.72 The Capability Extension File feature is used to modify certain NE capabilities without the need for a patch or software upgrade.

6.73 A Capability Extension File can add and/or remove supported pluggable transceivers in the mTera system. This allows new part numbers and functionality to be defined without requiring a software upgrade.

Overview

6.74 When upgrading to a new feature package a configuration file is applied during the upgrade.

6.75 When installing a new configuration file system must perform a check to verify feature package compatibility

6.76 Updating the Supported Pluggables list is accomplished in two basic steps:

- Capability Extension File Delivery: Transfers a zip file containing the pluggable transceiver file to the NE.
- Capability Extension File Installation: Unzips and installs pluggable transceiver files.

6.77 Each Revision of the Pluggable Transceiver File is identified by a pluggable transceiver version number.

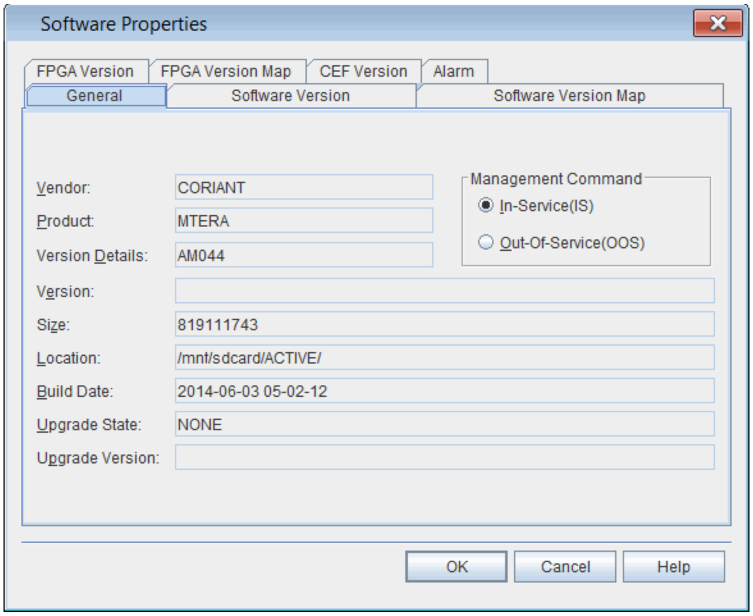
6.78 Pluggable Transceiver File does not support the concept of "fallback". You can, however, transfer a previous version of the pluggable transceiver file to the NE and load it, which would allow a customer to go back to the previously supported list if needed. There should not be a check to make sure that the version number is greater than the previous version number.

Verifying CEF Properties

6.79 Before downloading a capability file, verify that an upgrade is not currently taking place by performing the following steps.

__ 1. In the **Navigation Window**, right-click the **SW-1 - Software** icon to view the shortcut menu, then click **Properties**. The **Software Properties** dialog box displays. Refer to Figure 6.52, page 15-100.

Figure 6.52 Software Properties



Vendor:	CORIANT
Product:	MTERA
Version Details:	AM044
Version:	
Size:	819111743
Location:	/mnt/sdcard/ACTIVE/
Build Date:	2014-06-03 05-02-12
Upgrade State:	NONE
Upgrade Version:	

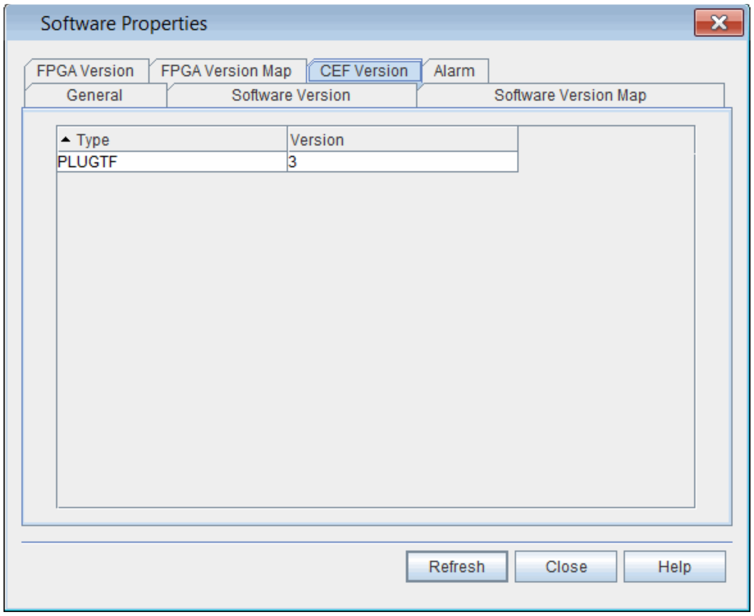
Management Command
● In-Service(IS)
○ Out-Of-Service(OOS)

__ 2. Verify that the **General** tab is selected.

__ 3. Verify that the **Upgrade State** is **NONE**, indicating than an upgrade is not currently running.

__ 4. Click the **CEF Version** tab. Refer to Figure 6.53, page 15-101.

Figure 6.53 Software Properties, CEF Version



Type	Version
PLUGTF	3

__ 5. The **CEF Version** contains information about the capability extension file versions for modules in the NE. Verify the following information:

- **Type** - type of CEF
- **Version** - CEF version

__ 6. Click **Close**.

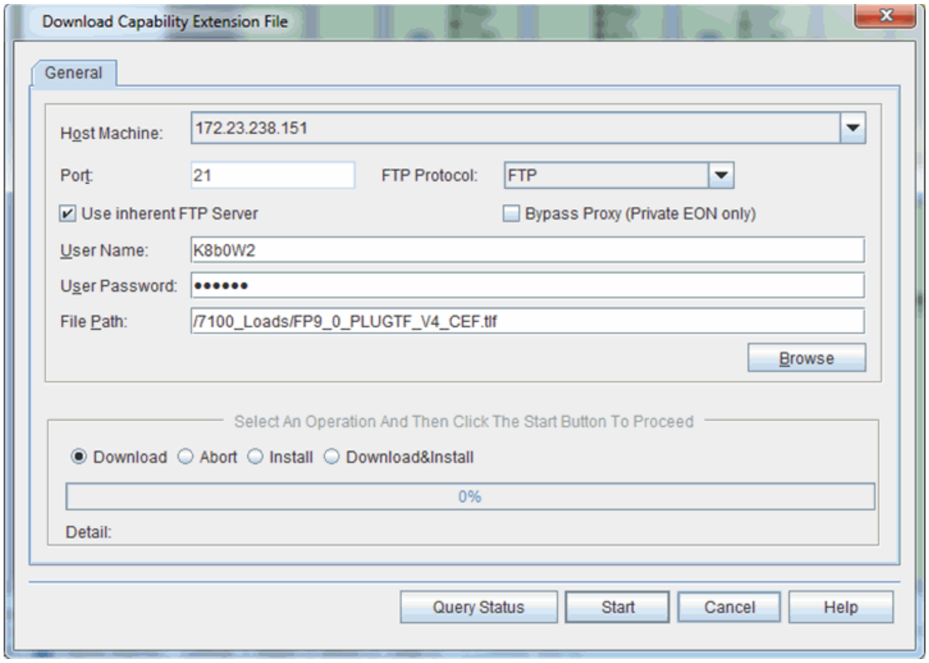
6.80 Review the current NE and module status information, review the *FP1.0.x Software Release Document*, and follow your company's prescribed procedures to determine if a capability extension file upgrade is needed.

Downloading Capability Extension File

6.81 Download a capability extension file by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **SW-1 - Software** icon to view the shortcut menu, then click **Download Capability Extension File**. The **Download Capability Extension File** dialog box displays. Refer to Figure 6.54, page 15-102.

Figure 6.54 Download Capability Extension File



Host Machine: 172.23.238.151

Port: 21 FTP Protocol: FTP

☑ Use inherent FTP Server □ Bypass Proxy (Private EON only)

User Name: K8b0W2

User Password: ••••••

File Path: /7100_Loads/FP9_0_PLUGTF_V4_CEF.tif

Select An Operation And Then Click The Start Button To Proceed

● Download ○ Abort ○ Install ○ Download&Install

0%

Detail:

6.82 Download and apply module software upgrade files by performing the following steps:

__ 1. Type the IP address of the **Host Machine** (FTP server) where the upgrade software is located.

__ 2. Type the communication **Port** for the software download.

__ 3. Click the **FTP Protocol** drop-down box to select **FTP** (file transfer protocol) or **SFTP** (secure file transfer protocol).

__ 4. The Craft Station provides an inherent **FTP** server for file transfers to the NE. An FTP server may also be running on the PC (refer to Setting Up FTP, page 15-12). If you intend to use the Craft Station FTP server for the software download, click **Use inherent FTP Server**.

__ 5. Leave the **Bypass Proxy (Private EON only)** box unchecked.

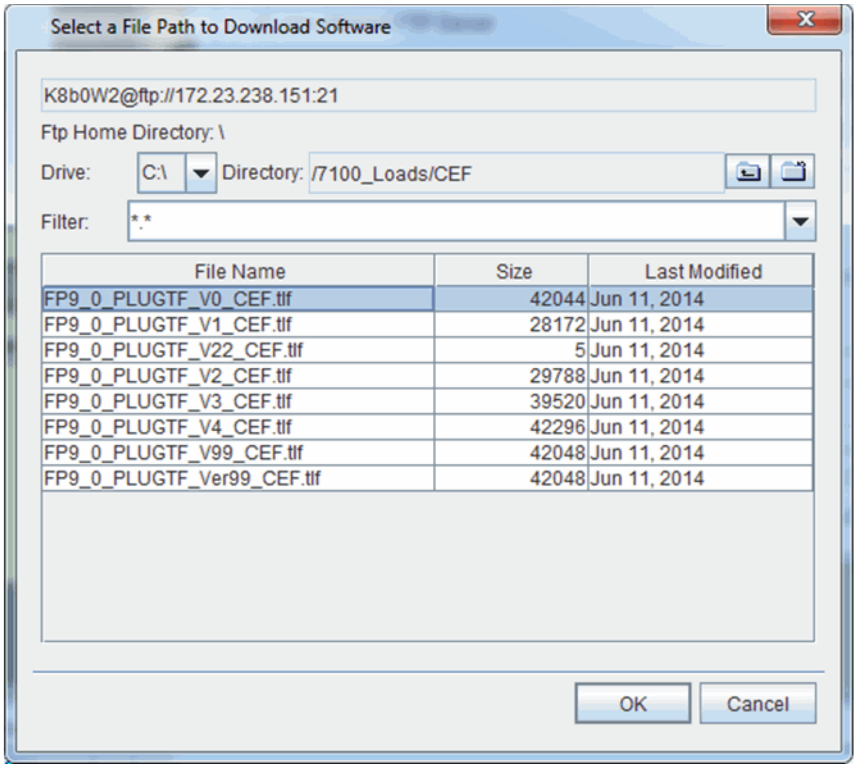
__ 6. Type the **User Name** required to access the FTP server where the new software is located. (The system automatically populates the **User Name** box if you selected Use inherent FTP Server.)

__ 7. Type the **User Password** required to access the FTP server where the new software is located. (The system automatically populates the **User Password** box if you selected Use inherent FTP Server.)

__ 8. Browse to, or type, the **File Path** where the CEF upgrade files are located on the FTP server. Refer to Figure 6.55, page 15-103.

Note: *If the Craft Station does not have IP connectivity to the FTP server, you must type the file path manually instead of using the browse button.*

Figure 6.55 Select a File Path to Download Software



Select a File Path to Download Software

K8b0W2@ftp://172.23.238.151:21

Ftp Home Directory: \

Drive: C:\ Directory: /7100_Loads/CEF

Filter: *.*

File Name	Size	Last Modified
FP9_0_PLUGTF_V0_CEF.tlf	42044	Jun 11, 2014
FP9_0_PLUGTF_V1_CEF.tlf	28172	Jun 11, 2014
FP9_0_PLUGTF_V22_CEF.tlf	5	Jun 11, 2014
FP9_0_PLUGTF_V2_CEF.tlf	29788	Jun 11, 2014
FP9_0_PLUGTF_V3_CEF.tlf	39520	Jun 11, 2014
FP9_0_PLUGTF_V4_CEF.tlf	42296	Jun 11, 2014
FP9_0_PLUGTF_V99_CEF.tlf	42048	Jun 11, 2014
FP9_0_PLUGTF_Ver99_CEF.tlf	42048	Jun 11, 2014

__ 9. Click to highlight target CEF file.

__ 10. Click **OK**. The **Select a File Path to Download Software** dialog box closes and the **Download Software Patch** dialog box returns.

Note: *During the patch application process, the active controller in a remote main shelf replicates the upgrade file from the active controller in the primary main shelf. The system generates a REPLUNIT-MISS (replaceable unit missing) alarm as the active controller in the remote main shelf under goes a warm start.*

__ 11. Perform the Download and Apply in two separate steps by going to substep 11.1, page 15-114. Or, perform the Download and Apply in one step by going to step 12, page 15-115.

__ 11.1 **Download** — Click this selection to copy the software from the server to the STPM. Click **Start**.

Depending on the size of the file, this step can take up to 20 minutes to complete. The download of the file is complete when the status bar indicates 100%.

When the system completes the module software patch download, a message displays at the bottom of the Download Software Patch dialog box.

__ 11.2 **Apply** — Click this selection to write the new software to the controller module (STPM).

Depending on the size of the file, this step can take up to 20 minutes to complete.

__ 11.3 Click **Start**.

__ 11.4 A **Confirmation** box displays stating that you are about to apply the patch. Click **OK**. The application of the patch is complete when status bar indicates 100%.

Depending on the size of the file, this step can take up to 20 minutes to complete.

__ 12. Perform the Download and Apply by performing the following step:

__ 12.1 **Download & Apply** (replaces substep 11.1, page 15-114 and substep 11.2, page 15-114) — Click this selection to perform Download and Apply in sequence and without user intervention. Click **Start**.

Depending on the size of the file, this step can take up to 50 minutes. The download and application of the file is complete when the status bar indicates 100%.

__ 13. It is possible to abort the download process. If necessary, click **Abort**, then click **Start** to stop the download.

__ 14. If necessary, click **Query Status** to open a dialog box that shows the current state of the download and application of the module software patch. (PATCHDELVIP = Patch Delivery In-Progress, PATCHDELVCOMPLD = Patch Delivery Completed, PATCHAPPLYIP = Patch Apply in Progress)

Verifying CEF Upgrade

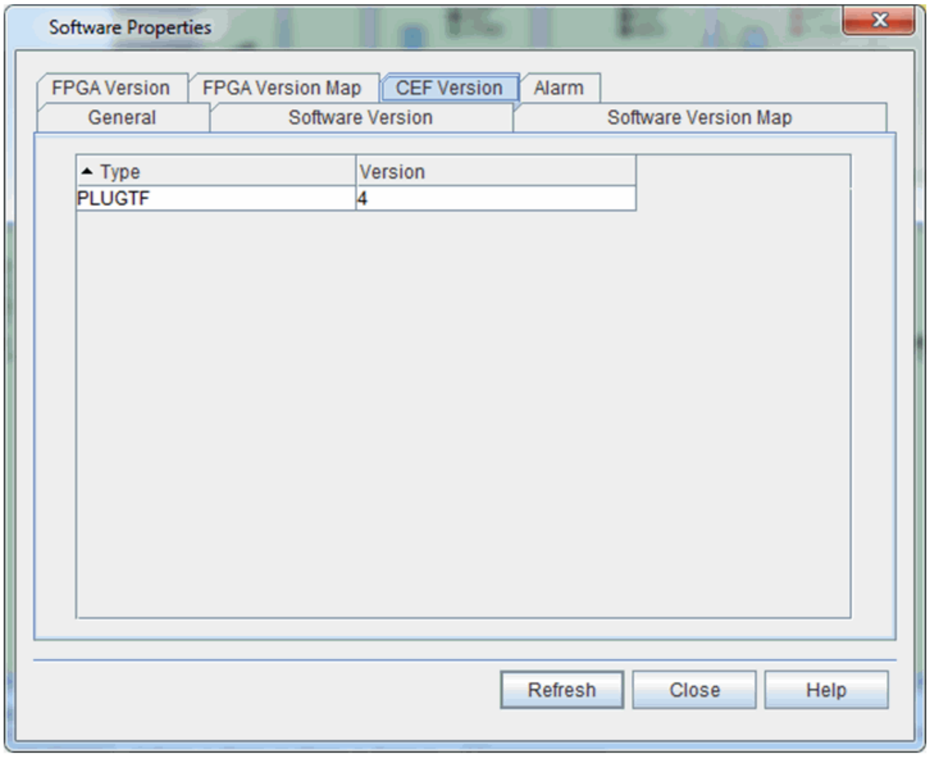
6.83 Verify that the CEF is complete by checking the CEF versions.

6.84 Verify the module software versions by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **SW-1 - Software** icon to view the shortcut menu, then click **Properties**. The **Software Properties** dialog box displays.

__ 2. Click the **CEF Version** tab. Refer to Figure 6.67, page 15-119.

Figure 6.56 Software Properties, CEF Version Tab, Post-Initialization



Type	Version
PLUGTF	4

__ 3. Verify that the **VERSION** number incremented by one for each module affected by the CEF upgrade.

__ 4. If necessary, click **Refresh** to update the patch level and status information.

__ 5. Click **OK**.

Module Software Upgrade

6.85 The module software upgrade feature allows you to update the software and/or firmware on an individual module–without the need to perform a complete software upgrade of the NE. This procedure describes how to download, apply, and initiate a module software upgrade.

6.86 Refer to *FP1.0.x NE Software Release Document* for the most current software/firmware patch levels per module.

Module Software Upgrade Overview

6.87 Coriant recommends the following sequence for upgrading module software and firmware:

__ 1. NE and Module Status - review NE and module software and firmware properties to determine necessary module upgrades.

__ 2. Patch Delivery - copies the patch load package from the server to the NE controller module.

__ 3. Patch Application - unzips and installs the patch software onto the processor module making the individual module software/firmware update available for upgrade to a specific module.

__ 4. Module Initialization - installs and commits the patch software or firmware to the individual module by performing either a software restart or cold restart.

__ 5. Patch Verification - confirms the module software upgrade is complete.

Note 1: *You can abort the module software upgrade procedure at any point before the patch is applied to the NE processor module. If you abort the application of the patch file, the original software and database are maintained for the module. The system deletes the patch file. Once the patch apply process has started, you must back out of the module software upgrade. Refer to Reverting to Previous Module Software and Firmware Version, page 15-121.*

Note 2: *Initializing module software on packet-enabled modules impacts traffic on all packet-enabled modules in the same shelf.*

Note 3: *A warm restart, cold restart/firmware patch, software patch, or upgrade of the packet-enabled modules requires a database download to refresh the Layer 2 configuration. During the database download the facilities may appear operationally ready but will not be configured properly with a traffic-enabling configuration until the database download is complete. This process typically takes 1 to 3 minutes but may take as long as 20 minutes due to database complexity or if there is significant activity on the system.*

Note 4: *Once a patch is applied to an NE, the NE automatically updates the software and firmware of a new module that is inserted in the NE.*

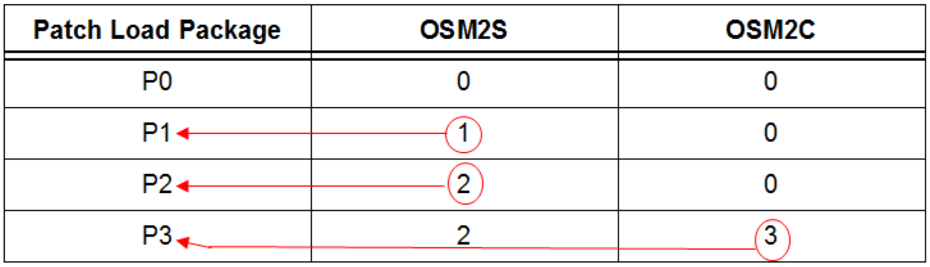
Patch Load Package

6.88 Software and firmware patch files for each module type to be patched are bundled into a patch load package (dcr and zip file). The patch load package contains only module patch files for the modules that have changed software or firmware since the initial feature package release.

6.89 Each patch load package is identified by a patch load number (P1, P2, P3, etc.) An example patch load filename is FP6_2_3_UZ123_20121022_P7. Only one patch load package can be installed on an NE at a time. Module patches are cumulative; therefore, a new module patch contains changes from the previous patch.

6.90 Module software upgrades or patches are managed by a software patch level that is unique to a feature package. Each new module software patch contains changes from the previous module software patch. Refer to Table 6.2, page 15-107 for example patch load package and module software numbering.

Table 6.2 Module Software Patch Level Example



Patch Load Package	OSM2S	OSM2C
P0	0	0
P1	1	0
P2	2	0
P3	2	3

6.91 Module firmware or FPGA patches are identified by a firmware version number for each field programmable device on a module.

6.92 The module software and firmware upgrade is only applied to a module if the current software patch level or firmware version for that module does not match the most current patch level. Refer to the *FP1.0.x NE Software Release Document* for the most current software/firmware patch levels per module type.

6.93 To remove or back out of a module software upgrade, a separate backout patch load package must be installed on the NE. An example backout patch load filename is FP9_0_3_UZ123_20121022_UNDO_1. This backout patch load package contains the necessary files to return to the firmware and software patch files stored on the NE to an unpatched state (patch level 0). If the module was at a patch level other than patch level 0, a module software upgrade needs to be performed with the appropriate patch level load package to return the module software to that patch level.

Upgrading Module Software on Controller Modules

6.94 This section describes special considerations when upgrading module software on system processor modules.

Verifying Active and Standby Status

6.95 Verify the active and standby status of the STPMs by performing the following steps. From the **Navigation Window**, right-click the module to view the shortcut menu, then click **Properties**. The **Properties** dialog box displays. Click the **State** tab. Verify the active or standby status of the controller in the **Secondary State** box.

Upgrading Standby Controller First

6.96 When upgrading STPMs, follow the software upgrade procedure for the Standby controller first. Execute the INIT-SYS PH5 to load the patch, then force a switch of the active and standby status of the controllers. Repeat the procedure when the switch completes.

Upgrade All Controller Modules in NE to Same Module Software Release

6.97 When performing a module software upgrade on the STPM, upgrade each system processor module the shelf to the same module software release.

Module Software Upgrade Prerequisites

6.98 Confirm the following conditions are in place before beginning the module software upgrade.

__ The module upgrade software (patch load package) is copied from the DVD to an FTP server that is accessible before starting the module software upgrade. Refer to the *FP1.0.x NE Software Release Document* to verify you have the correct patch load package for the specific module software upgrade.

__ The NE hardware components meet the baseline requirements for the upgrade software release. Refer to the *FP1.0.x NE Software Release Document* for these requirements.

__ The communication links between the various elements involved in the upgrade are fully operational.

__ All system provisioning activity has stopped for the NE.

__ A user with NE administrator privileges is logged into the system to perform the module software upgrade.

__ A backup NE database has been made to a remote server.

__ The NE is in a stable state and is operating normally.

__ All equipment alarms and conditions are cleared prior to the start of the upgrade.

Note 1: *If the equipment alarms and conditions do not clear, follow your company's prescribed procedures for obtaining technical assistance, or contact the Coriant Technical Assistance Center at http://www.coriant.com/services_support/.*

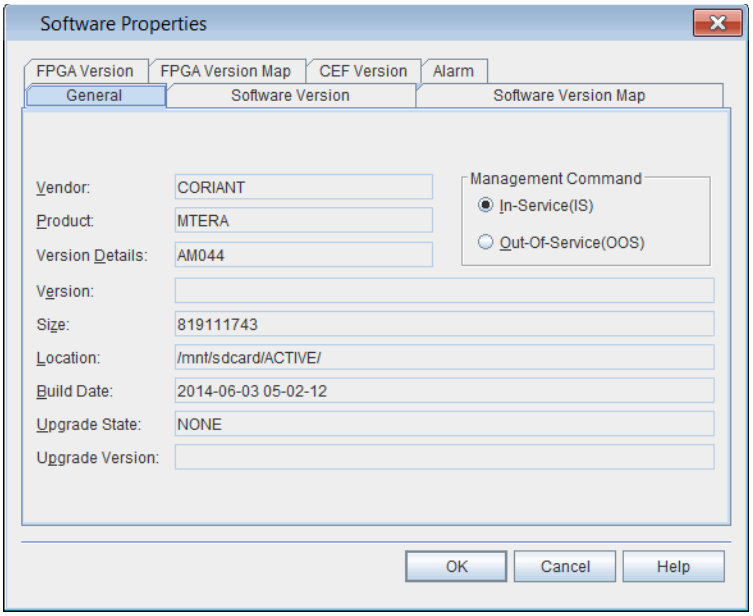
Note 2: *Stop the upgrade procedure at any point before the patch is applied to the system processor module by clicking **Abort**. If you abort the application of the patch file, the original software and database are maintained for the module. The system deletes the patch file.*

Verifying NE Software and Module Software Properties

6.99 Before downloading a module software patch file, verify that an upgrade is not currently taking place by performing the following steps.

__ 1. In the **Navigation Window**, right-click the **SW-1 - Software** icon to view the shortcut menu, then click **Properties**. The **Software Properties** dialog box displays. Refer to Figure 6.57, page 15-109.

Figure 6.57 Software Properties



Vendor: CORIANT

Product: MTERA

Version Details: AM044

Version:

Size: 819111743

Location: /mnt/sdcard/ACTIVE/

Build Date: 2014-06-03 05-02-12

Upgrade State: NONE

Upgrade Version:

Management Command

● In-Service(IS)

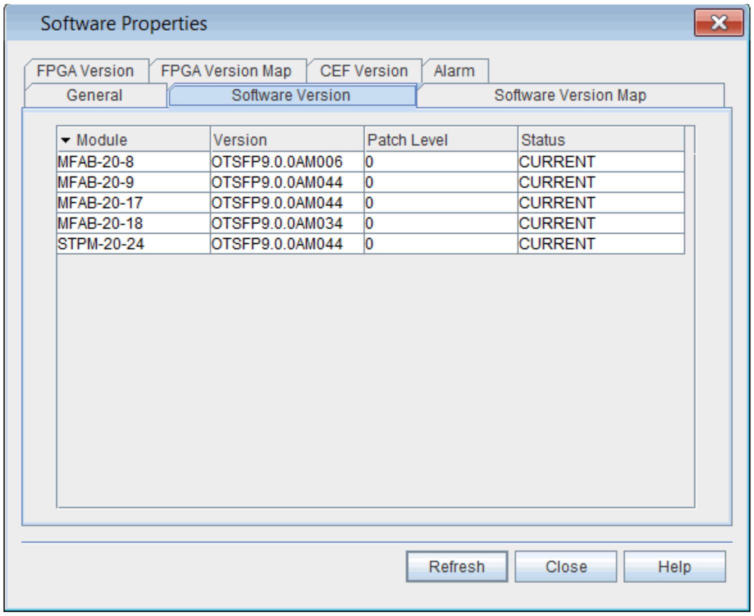
○ Out-Of-Service(OOS)

__ 2. Verify that the **General** tab is selected.

__ 3. Verify that the **Upgrade State** is **NONE**, indicating than an upgrade is not currently running.

__ 4. Click the **Software Version** tab. Refer to Figure 6.58, page 15-109.

Figure 6.58 Software Properties, Software Version Tab



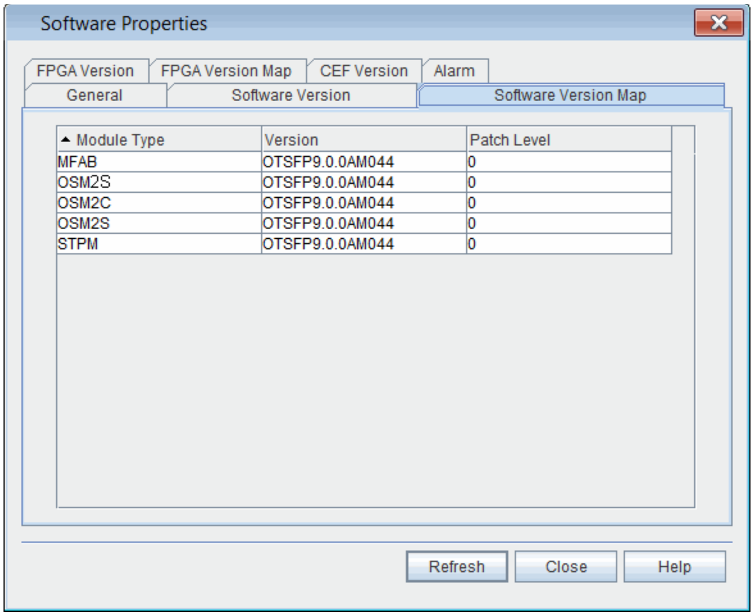
Module	Version	Patch Level	Status
MFAB-20-8	OTSFP9.0.0AM006	0	CURRENT
MFAB-20-9	OTSFP9.0.0AM044	0	CURRENT
MFAB-20-17	OTSFP9.0.0AM044	0	CURRENT
MFAB-20-18	OTSFP9.0.0AM034	0	CURRENT
STPM-20-24	OTSFP9.0.0AM044	0	CURRENT

__ 5. The **Software Version** tab lists the software versions and patch levels of each module in the NE. Verify the following information:

- **Module** - module name, shelf number, and slot number
- **Version** - software version currently running on the module
- **Patch Level** - software patch level installed and running on the module. Patch level 0 is the initial feature package release (no patches).
- **Status** - NOT CURRENT if module has out-of-date software version, CURRENT if module has up-to-date software version

__ 6. Click the **Software Version Map** tab. Refer to Figure 6.59, page 15-110.

Figure 6.59 Software Properties, Software Version Map Tab



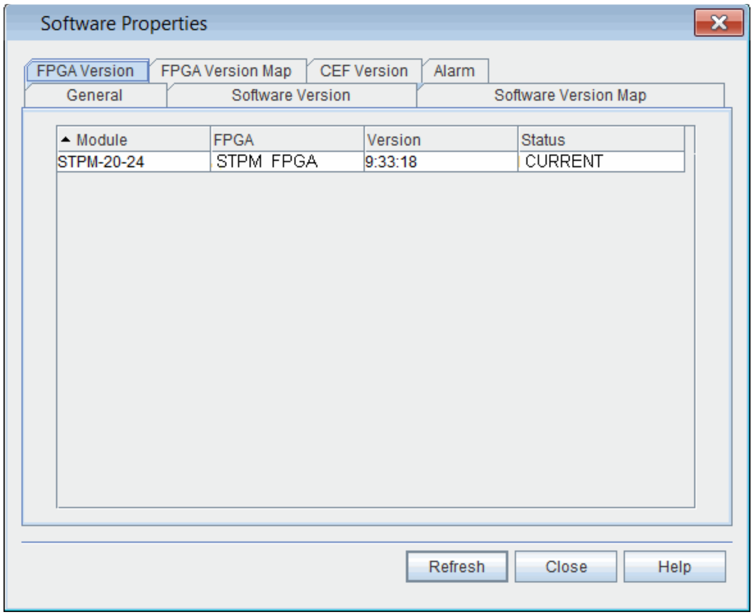
Module Type	Version	Patch Level
MFAB	OTSFP9.0.0AM044	0
OSM2S	OTSFP9.0.0AM044	0
OSM2C	OTSFP9.0.0AM044	0
OSM2S	OTSFP9.0.0AM044	0
STPM	OTSFP9.0.0AM044	0

__ 7. The **Software Version Map** lists the patch levels and software versions of modules available in the NE. Verify the following information:

- **Module Type** - type of module
- **Version** - software version associated with patch level
- **Patch Level** - latest software patch level available for module type

__ 8. Click the **FPGA Version** tab. Refer to Figure 6.60, page 15-111.

Figure 6.60 Software Properties, FPGA Version Tab



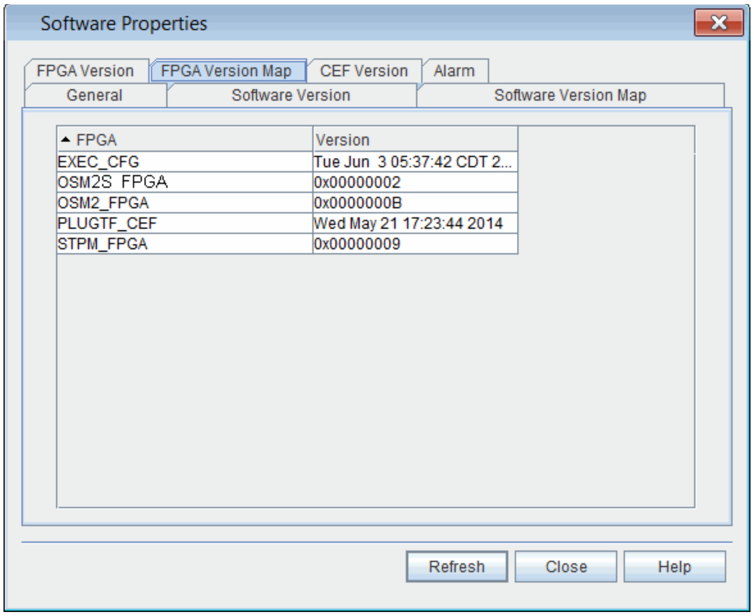
Module	FPGA	Version	Status
STPM-20-24	STPM FPGA	9:33:18	CURRENT

__ 9. The **FPGA Version** tab contains information about the firmware for modules that support a field programmable gate array. Verify the following information:

- **Module** - module AID
- **FPGA** - name of FPGA
- **Version** - FPGA version
- **Status** - NOT CURRENT if module has out-of-date FPGA version, CURRENT if module has up-to-date FPGA version

__ 10. Click the **FPGA Version Map** tab. Refer to Figure 6.61, page 15-111.

Figure 6.61 Software Properties, FPGA Version Map Tab



FPGA	Version
EXEC_CFG	Tue Jun 3 05:37:42 CDT 2...
OSM2S FPGA	0x00000002
OSM2_FPGA	0x0000000B
PLUGTF_CEF	Wed May 21 17:23:44 2014
STPM_FPGA	0x00000009

__ 11. The **FPGA Version Map** contains information about the FPGA versions for modules in the NE. Verify the following information:

- **FPGA** - FPGA name
- **Version** - firmware version

__ 12. Click **Close**.

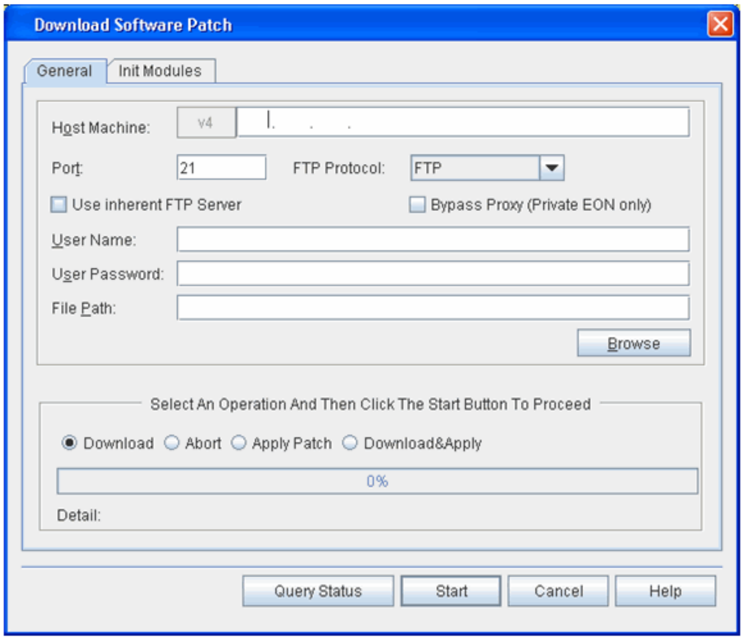
6.100 Review the current NE and module status information, review *FP1.0.x Software Release Document*, and follow your company's prescribed procedures to determine if a module software or firmware upgrade is needed.

Downloading Module Software Upgrade File

6.101 Download a module software upgrade file by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **SW-1 - Software** icon to view the shortcut menu, then click **Download Software Patch**. The **Download Software Patch** dialog box displays. Refer to Figure 6.62, page 15-112.

Figure 6.62 Download Software Patch



Download Software Patch

General | Init Modules

Host Machine: v4

Port: 21 FTP Protocol: FTP

☐ Use inherent FTP Server ☐ Bypass Proxy (Private EON only)

User Name:

User Password:

File Path:

Select An Operation And Then Click The Start Button To Proceed

● Download ○ Abort ○ Apply Patch ○ Download&Apply

0%

Detail:

6.102 Download and apply module software upgrade files by performing the following steps:

__ 1. Type the IP address of the **Host Machine** (FTP server) where the upgrade software is located.

__ 2. Type the communication **Port** for the software download.

__ 3. Click the **FTP Protocol** drop-down box to select **FTP** (file transfer protocol) or **SFTP** (secure file transfer protocol).

__ 4. The Craft Station provides an inherent **FTP** server for file transfers to the NE. An FTP server may also be running on the PC (refer to Setting Up FTP, page 15-12). If you intend to use the Craft Station FTP server for the software download, click **Use inherent FTP Server**.

__ 5. Leave the **Bypass Proxy (Private EON only)** box unchecked.

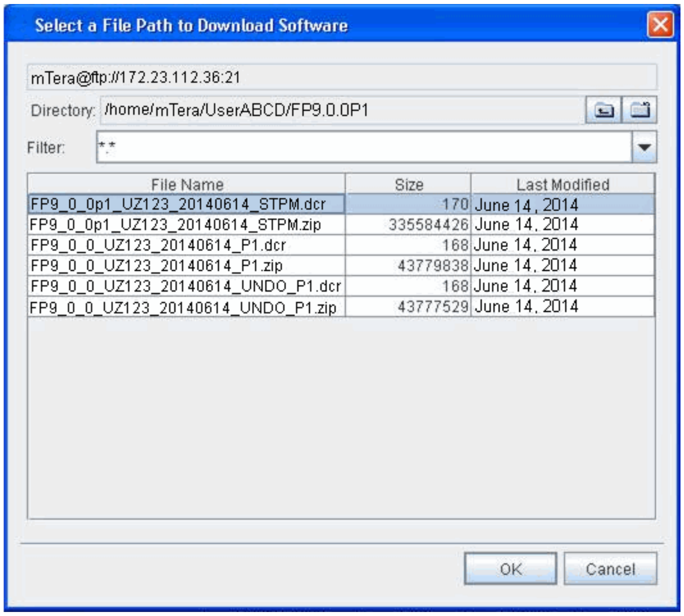
__ 6. Type the **User Name** required to access the FTP server where the new software is located. (The system automatically populates the **User Name** box if you selected Use inherent FTP Server.)

__ 7. Type the **User Password** required to access the FTP server where the new software is located. (The system automatically populates the **User Password** box if you selected Use inherent FTP Server.)

__ 8. Browse to, or type, the **File Path** where the software upgrade files are located on the FTP server. Refer to Figure 6.63, page 15-113.

Note: *If the Craft Station does not have IP connectivity to the FTP server, you must type the file path manually instead of using the browse button.*

Figure 6.63 Select a File Path to Download Software



mTera@ftp://172.23.112.36:21

Directory: /home/mTera/UserABCD/FP9.0.0P1

Filter: *.*

File Name	Size	Last Modified
FP9_0_0p1_UZ123_20140614_STPM.dcr	170	June 14, 2014
FP9_0_0p1_UZ123_20140614_STPM.zip	335584426	June 14, 2014
FP9_0_0_UZ123_20140614_P1.dcr	168	June 14, 2014
FP9_0_0_UZ123_20140614_P1.zip	43779838	June 14, 2014
FP9_0_0_UZ123_20140614_UNDO_P1.dcr	168	June 14, 2014
FP9_0_0_UZ123_20140614_UNDO_P1.zip	43777529	June 14, 2014

__ 9. Click to highlight the dcr and zip files for the module software patch.

__ 10. Click **OK**. The **Select a File Path to Download Software** dialog box closes and the **Download Software Patch** dialog box returns.

Note: *During the patch application process, the active controller in a remote main shelf replicates the upgrade file from the active controller in the primary main shelf. The system generates a REPLUNIT-MISS (replaceable unit missing) alarm as the active controller in the remote main shelf under goes a warm start.*

__ 11. Perform the Download and Apply in two separate steps by going to substep 11.1, page 15-114. Or, perform the Download and Apply in one step by going to step 12, page 15-114.

__ 11.1 **Download** — Click this selection to copy the software from the server to the SPM or SPM-N. Click **Start**.

Depending on the size of the file, this step can take up to 20 minutes to complete. The download of the file is complete when the status bar indicates 100%.

When the system completes the module software patch download, a message displays at the bottom of the Download Software Patch dialog box.

__ 11.2 **Apply** — Click this selection to write the new software to the controller module (SPM or SPM-N).

Depending on the size of the file, this step can take up to 20 minutes to complete.

__ 11.3 Click **Start**.

__ 11.4 A **Confirmation** box displays stating that you are about to apply the patch. Click **OK**. The application of the patch is complete when status bar indicates 100%.

Depending on the size of the file, this step can take up to 20 minutes to complete.

__ 12. Perform the Download and Apply by performing the following step:

__ 12.1 **Download & Apply** (replaces substep 11.1, page 15-114 and substep 11.2, page 15-114) — Click this selection to perform Download and Apply in sequence and without user intervention. Click **Start**.

Depending on the size of the file, this step can take up to 50 minutes. The download and application of the file is complete when the status bar indicates 100%.

__ 13. It is possible to abort the download process. If necessary, click **Abort**, then click **Start** to stop the download.

__ 14. If necessary, click **Query Status** to open a dialog box that shows the current state of the download and application of the module software patch. (PATCHDELVIP = Patch Delivery In-Progress, PATCHDELVCOMPLD = Patch Delivery Completed, PATCHAPPLYIP = Patch Apply in Progress)

Verifying Available Module Software Level and FPGA Version

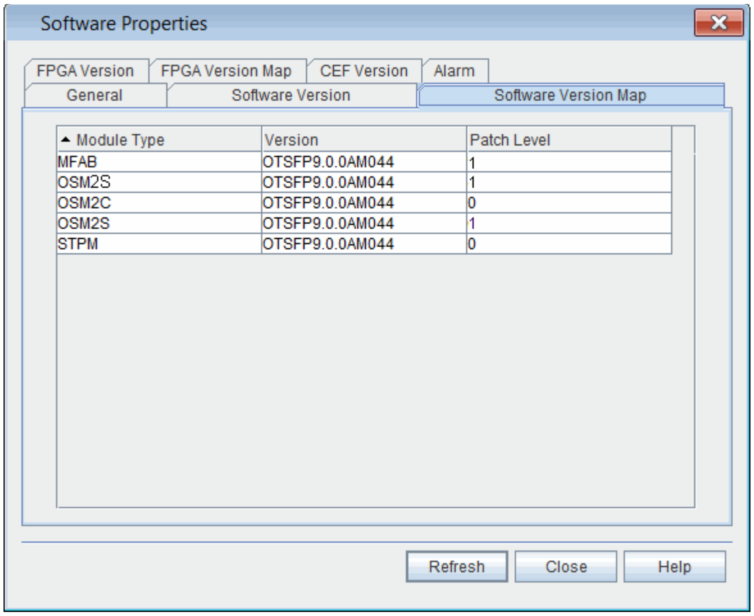
6.103 After downloading and applying the file, verify the updates available for each module.

6.104 Verify the available software patch level by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **SW-1 - Software** icon to view the shortcut menu, then click **Software Properties**. The **Software Properties** dialog box displays.

__ 2. Click the **Software Version Map** tab. Refer to Figure 6.64, page 15-115.

Figure 6.64 Software Properties, Software Version Map Tab, Post-Patch Download and Application



Module Type	Version	Patch Level
MFAB	OTSFP9.0.0AM044	1
OSM2S	OTSFP9.0.0AM044	1
OSM2C	OTSFP9.0.0AM044	0
OSM2S	OTSFP9.0.0AM044	1
STPM	OTSFP9.0.0AM044	0

__ 3. Review the available patch level for each module in the **Patch Level** column.

__ 4. If necessary, click **Refresh** to update the table.

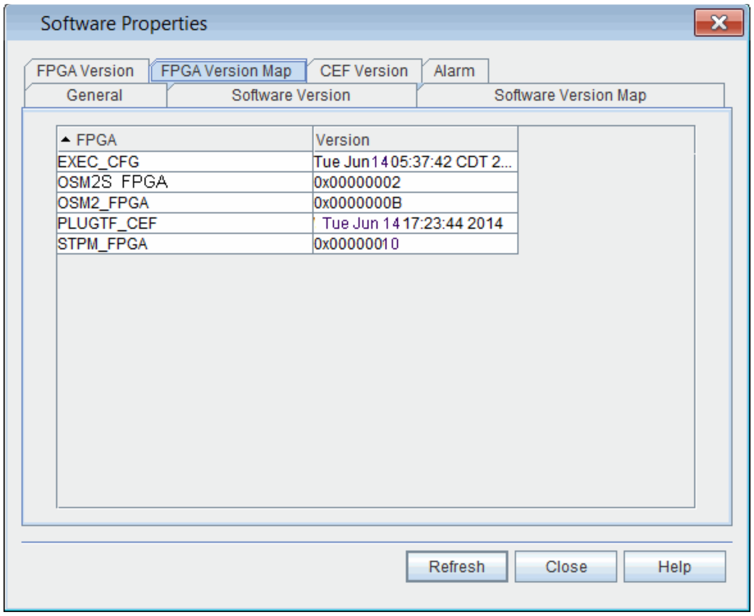
__ 5. Click **Close**.

6.105 Verify the available FPGAs by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **SW-1 - Software** icon to view the shortcut menu, then click **Software Properties**. The **Software Properties** dialog box displays.

__ 2. Click the **FPGA Version Map** tab. Refer to Figure 6.65, page 15-116.

Figure 6.65 Software Properties, FPGA Version Map Tab, Post-Patch Download and Application



▲ FPGA	Version
EXEC_CFG	Tue Jun 14 05:37:42 CDT 2...
OSM2S FPGA	0x00000002
OSM2_FPGA	0x0000000B
PLUGTF_CEF	Tue Jun 14 17:23:44 2014
STPM_FPGA	0x00000010

__ 3. Review the names of the available FPGAs in the **FPGA** column.

__ 4. Review the available FPGA versions in the **Version** column.

__ 5. If necessary, click **Refresh** to update the table.

__ 6. Click **Close**.

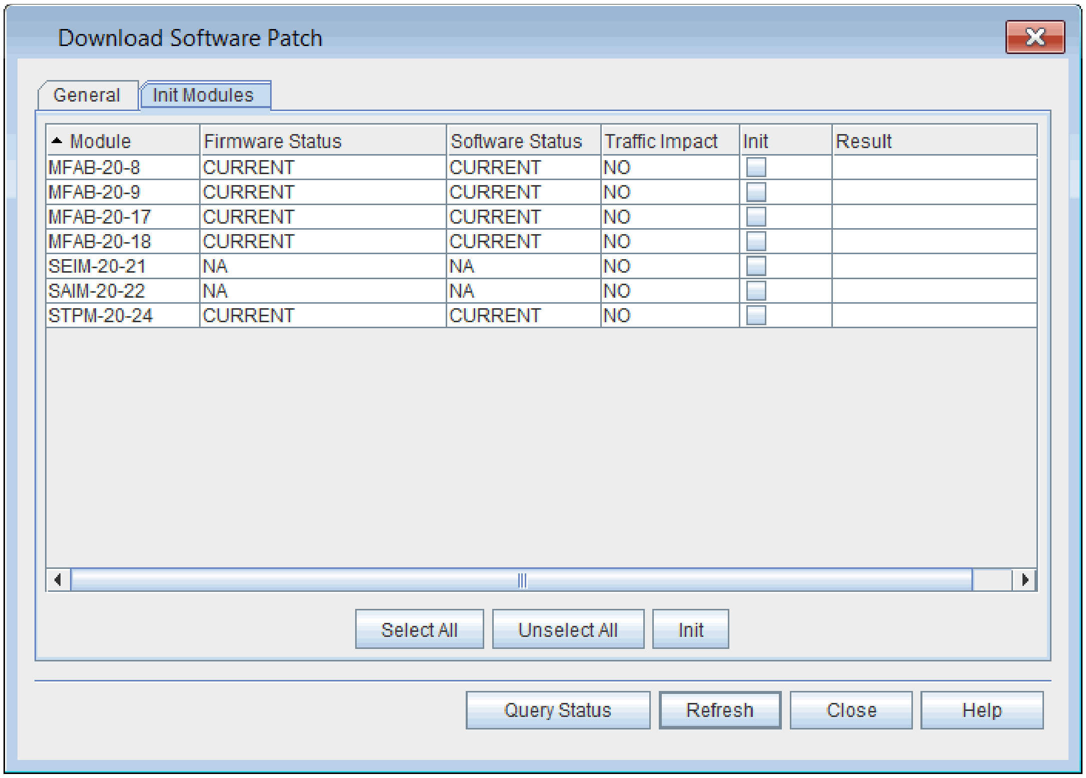
Initializing Module Software

6.106 If you are initializing an STPM, first initialize the standby controller. Next, switch controllers from the active to standby. Then, repeat the process and initialize the active controller.

6.107 Initialize the module software and/or firmware by performing the following steps:

__ 1. In the **Download Software Patch** dialog box, click the **Init Modules** tab. Refer to Figure 6.66, page 15-117.

Figure 6.66 Download Software Patch, Init Modules Tab



Module	Firmware Status	Software Status	Traffic Impact	Init	Result
MFAB-20-8	CURRENT	CURRENT	NO	□	
MFAB-20-9	CURRENT	CURRENT	NO	□	
MFAB-20-17	CURRENT	CURRENT	NO	□	
MFAB-20-18	CURRENT	CURRENT	NO	□	
SEIM-20-21	NA	NA	NO	□	
SAIM-20-22	NA	NA	NO	□	
STPM-20-24	CURRENT	CURRENT	NO	□	

__ 2. Click **Refresh** to view the latest **Firmware Status** and **Software Status** for each module (**NOT CURRENT**, **CURRENT**, or **NA**).

Note: *It may take several minutes for the software status to update in the Download Software Patch, Init Modules tab.*

__ 3. Choose one of the following options:

- If you are initializing an STPM, go to substep 3.1, page 15-117.
- If you are initializing transponders, go to substep 3.2, page 15-117.

__ 3.1 Initialize the standby controller first. (After the software update completes, switch to the standby controller. Then repeat the procedure on the newly standby controller.)

You can initialize the standby controller, port modules, or the standby controller along with port modules at the same time. However, do not initialize the active and standby controller at the same time.

__ 3.2 In the **Init** column, select each module to which you want to apply the patch. Or, choose one of the following options:

- Click **Select All** to select each module in the NE.
- Click **Unselect All** to clear the list of modules targeted for patching.

Note: *If necessary, refer to the FP1.0.x NE Software Release Document to verify which modules are impacted by the software patch release.*

__ 4. Review the **Traffic Impact** column to determine if traffic will be impacted during the module initialization process.

__ 5. Click **Init**.

Note 1: *During the module initialization process, the system generates a REPLUNIT-MISS (replaceable unit missing) alarm as each module undergoes a software restart for the software update.*

Note 2: *If you are initializing an STPM, the system generates a PROTNA alarm on the active STPM.*

Note 3: *Upon module initialization, the system installs the software to the module. Then if a firmware patch update is available the system automatically begins the firmware update to that module. Performing a software restart on a module that requires both a software and firmware update results in an automatic cold restart, which is necessary to load the firmware. Depending on the size of the file, the firmware update may take up to 20 minutes to complete.*

__ 6. Click **Refresh** to track the progress of the module initialization process in the **Result** column. If the initialization process is successful, Initiated displays in the field. If the process is unsuccessful, an error message displays in the field.

__ 7. Click **Refresh** to track the progress of the module initialization process. The initialization is complete when the **Firmware Status** column and **Software Status** column display CURRENT for the applicable modules.

Note: *It may take several minutes for the software status to update in the Download Software Patch, Init Modules tab.*

Sequence of Alarms Displayed for STPM Software Upgrade

6.108 If you are initializing an STPM, note that the system displays the following alarms:

1. PROTNA on the active controller
2. REPLUNIT MISSING on standby controller; when you repeat procedure system displays REPLUNIT MISSING on the newly standby controller
3. DBSYNC on standby controller; when you repeat procedure system displays DBSYNC on the newly standby controller
4. the initialization is complete when the DBSYNC alarm clears on the standby controller; when you repeat procedure the initialization is complete when the DBSYNC alarm clears on the newly standby controller

Verifying Module Software and Firmware Upgrade

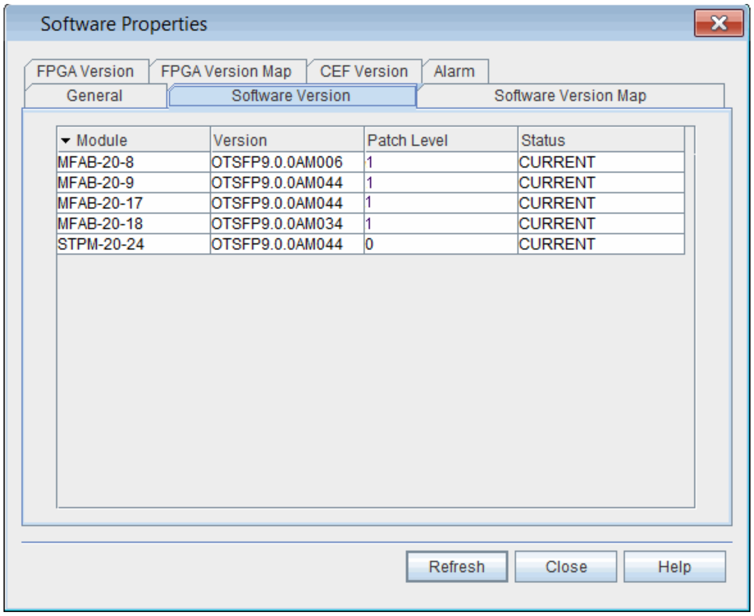
6.109 Verify that the module software upgrade is complete by checking the module software and firmware versions.

6.110 Verify the module software versions by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **SW-1 - Software** icon to view the shortcut menu, then click **Properties**. The **Software Properties** dialog box displays.

__ 2. Click the **Software Version** tab. Refer to Figure 6.67, page 15-119.

Figure 6.67 Software Properties, Software Version Tab, Post-Initialization



Module	Version	Patch Level	Status
MFAB-20-8	OTSFP9.0.0AM006	1	CURRENT
MFAB-20-9	OTSFP9.0.0AM044	1	CURRENT
MFAB-20-17	OTSFP9.0.0AM044	1	CURRENT
MFAB-20-18	OTSFP9.0.0AM034	1	CURRENT
STPM-20-24	OTSFP9.0.0AM044	0	CURRENT

__ 3. Verify that the **Patch Level** number incremented by one for each module affected by the software patch load.

__ 4. Verify that the Status is **CURRENT** for each module affected by the software patch load.

__ 5. If necessary, click **Refresh** to update the patch level and status information.

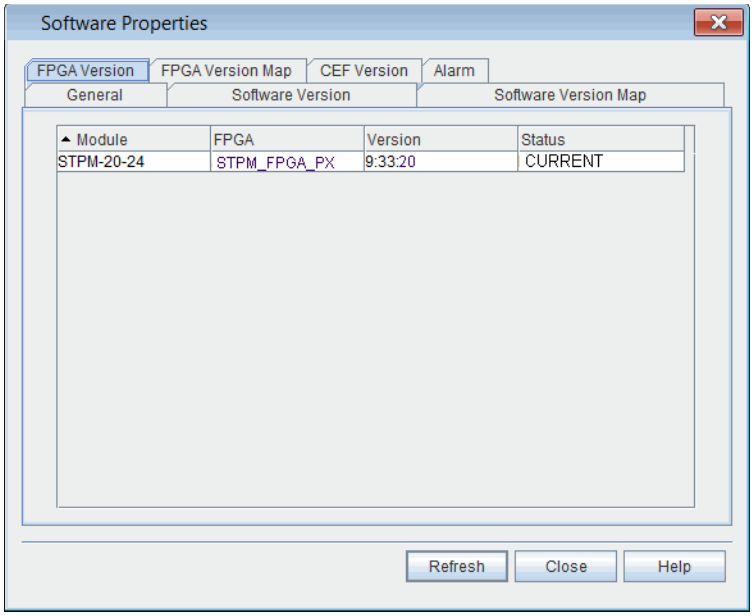
__ 6. Click **OK**.

6.111 Verify the firmware versions by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **SW-1 - Software** icon to view the shortcut menu, then click **Properties**. The **Software Properties** dialog box displays.

__ 2. Click the **FPGA Version** tab. Refer to Figure 6.68, page 15-120.

Figure 6.68 Software Properties, FPGA Version Tab, Post-Initialization



Module	FPGA	Version	Status
STPM-20-24	STPM_FPGA_PX	9:33:20	CURRENT

__ 3. Verify that the **Status** is **CURRENT** for each module affected by the software patch load.

__ 4. If necessary, click **Refresh** to update the patch level and status information.

__ 5. Click **OK**.

__ 6. Choose one of the following options:

- If you are upgrading transponders, the procedure is complete.
- If you are upgrading a controller module, go to Switching Controller Module, page 15-121.

Switching Controller Module

6.112 The initialization is complete when the DBSYNC alarm clears. When the DBSYNC alarm clears, switch to the standby controller by performing the following steps:

Note 1: *The management system loses NE visibility and TL1 connectivity while the STPMs switch between Active and Standby states. This lack of NE visibility and TL1 connectivity may last up to 20 minutes.*

Note 2: *In addition, the formerly active STPM may take 20 to 40 minutes to complete the SYNC process–depending on database complexity and activity on the system. The SYNC is complete when the PROTNA alarm against the newly active STPM clears.*

__ 1. In the **Navigation Window**, right-click the controller to view the shortcut menu, then click **Switch to Standby Controller**. A **Warning** message displays that states: "You are about to switch from ACTIVE to STANDBY controller. This Operation will disconnect all TL1 Active Sessions and cause a lost of NE visibility for a few minutes. Do you want to continue?"

__ 2. Click **Yes**.

Completing Module Software Upgrade on Controller Module

6.113 If you are performing a module software upgrade on a controller module, wait for the controller switch and software synchronization to complete. Then repeat Initializing Module Software, page 15-116 through Switching Controller Module, page 15-121 for the active controller.

Upgrade All Controller Modules in NE to Same Module Software Release

6.114 When performing a module software upgrade on an STPM, upgrade each controller module in all shelves of the NE to the same module software release.

Reverting to Previous Module Software and Firmware Version

6.115 If it is necessary to revert to module software and firmware version previously installed, perform the following steps:

6.116 Repeat Verifying NE Software and Module Software Properties, page 15-108 through Verifying Module Software and Firmware Upgrade, page 15-119 using the "undo" patch files contained in the software patch load. The "undo" files return the module software and FPGA to the version of the initial package release.

6.117 From there, a patch load package containing patch files of a previous patch level from what had been installed on the NE can loaded onto the system.

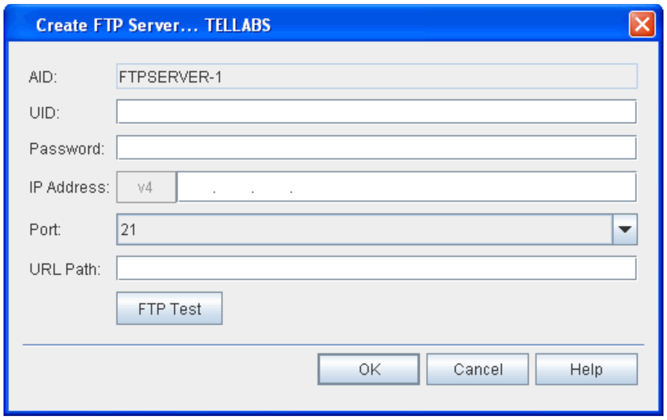
Creating an FTP Server

6.118 Define an FTP server so that you can export specific performance monitoring data files collected at the NE. Historical performance monitoring data is exported in binary format, requiring an FTP server. This section describes how to provision the server.

6.119 Create an FTP server by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NE** icon to view the shortcut menu, then click **Create FTP Server**. The **Create FTP Server** dialog box displays. Refer to Figure 6.69, page 15-122.

Figure 6.69 Create FTP Server



Create FTP Server... TELLABS

AID: FTPSERVER-1

UID:

Password:

IP Address: v4 . . .

Port: 21

URL Path:

__ 2. The **AID** box defaults to the next incremented number.

__ 3. In the **UID** box, type a user ID that is valid on the FTP server.

__ 4. In the **Password** box, type the password associated for the user defined in the previous step.

__ 5. In the **IP Address** box, type the IP address of the FTP server. (IPv4 or IPv6 IP address format).

__ 6. In the **Port** box, type the logical port number associated with the FTP server IP address.

__ 7. In the **URL Path** box, type the URL path of the FTP server where to store the files.

__ 8. Click **FTP Test** to test the FTP server.

__ 9. Click **OK**.

Managing Environmental Alarms

6.120 Provision up to four environmental alarms per NE. Manage environmental alarms on the system by performing the following steps:

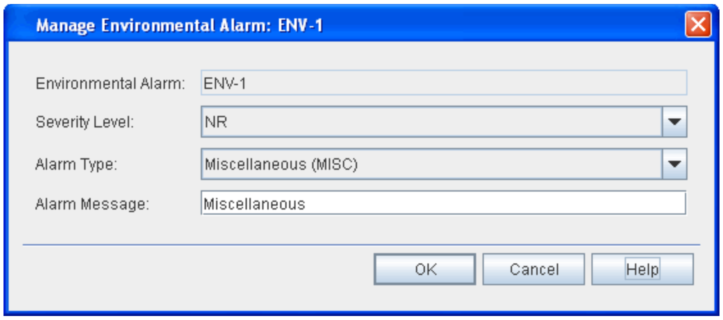
__ 1. In the **Navigation Window**, expand the **TELEMETRY** icon.

__ 2. Expand the **Environmental Alarms** icon.

__ 3. Right-click the **ENV-1** icon to view the shortcut menu, then click **Manage ENV**.

__ 4. The **Manage Environmental Alarms ENV-x** dialog box displays. Refer to Figure 6.70, page 15-123.

Figure 6.70 Manage Environmental Alarm



Manage Environmental Alarm: ENV-1

Environmental Alarm: ENV-1

Severity Level: NR

Alarm Type: Miscellaneous (MISC)

Alarm Message: Miscellaneous

__ 5. Select the severity to associate with the condition in the **Severity Level** drop-down box.

__ 6. Click the **Alarm Type** drop-down box to select an alarm to assign to this Environmental Alarm (**ENV-1**, **ENV-2**, **ENV-3**, and **ENV-4**). The alarm message assigned to the alarm type displays in the **Alarm Message** box.

Managing External Contacts

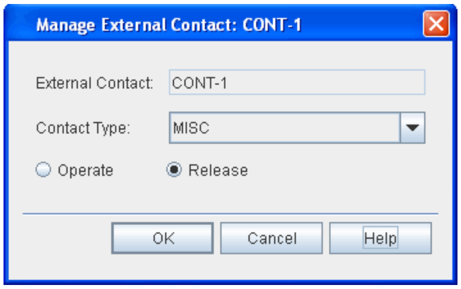
6.121 Follow the steps below to manage electrical contacts on equipment external to the NE. The NE supports up to four provisionable external contacts.

__ 1. In the **Navigation Window**, expand the **TELEMETRY** icon.

__ 2. Expand the **External Contacts** icon.

__ 3. Right-click the **CONT-x** icon to view the shortcut menu, then click **Manage CONT**. The **Manage External Contact: CONT-x** dialog box displays. Refer to Figure 6.71, page 15-123.

Figure 6.71 Manage External Contact



Manage External Contact: CONT-1

External Contact: CONT-1

Contact Type: MISC

○ Operate ● Release

__ 4. Click the **Contact Type** drop-down box to select the equipment to control.

__ 5. Click **Operate** or **Release** to change the state of the equipment. The icon next to the contact type in the **Navigation Window** shows the current state of the equipment.

7. Provisioning Network Element Settings

7.1 This section provides instructions for provisioning the network element (NE).

Note: *Refer to TL1 Command Reference Manual for supported network configurations, and additional details on network element settings. Click the Help menu in the Craft Station to access this document.*

Provisioning the NE

7.2 Define the NE and network type during NE commissioning. Refer to Commissioning an NE, page 15-11. Access this and other information on the NE via the **NE** icon in the **Navigation Window**.

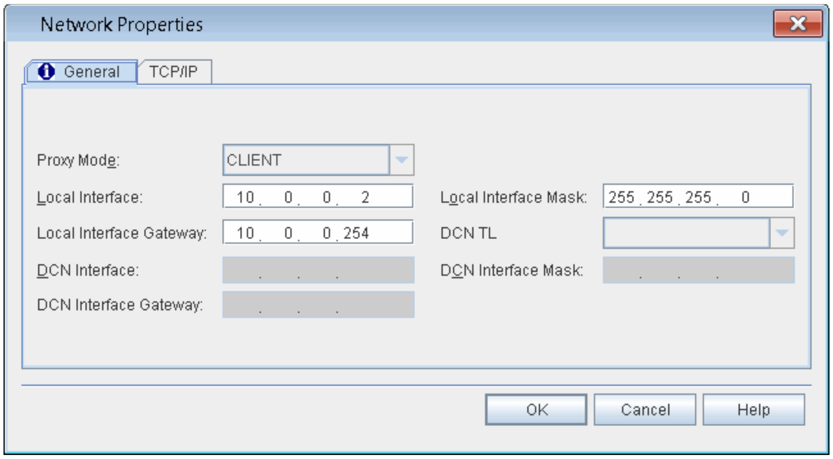
Viewing Network Properties

7.3 Access the NE menu and view the network properties by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NE** icon to view the shortcut menu, then click **Network Properties**. The **Network Properties** dialog box displays.

__ 2. Verify that the **General** tab is selected. Refer to Figure 7.1, page 15-124.

Figure 7.1 Network Properties



Proxy Mode: CLIENT

Local Interface: 10 . 0 . 0 . 2

Local Interface Mask: 255 . 255 . 255 . 0

Local Interface Gateway: 10 . 0 . 0 . 254

DCN TL

DCN Interface: . . .

DCN Interface Mask: . . .

DCN Interface Gateway: . . .

7.4 Active fields in this dialog box are specific to the type of EON selected. Fields that are not relevant to the selected topology appear grayed out. Refer to Table 7.1, page 15-125 for a description of the network properties field.

Table 7.1 Fields in Network Properties Dialog Box

Field	Definition
Proxy Mode	CLIENT
Local Interface	IP address of local craft port
Local Interface Gateway	Used to provision an external gateway of the LCI
Local Interface Mask	Mask for the external address for connection to the Local Craft port

Modifying State of NE

7.5 This section describes how to place an NE in-service or out-of-service.

Provisioning an NE In-Service

7.06 Place an NE in-service by performing the following steps:

— 1. In the **Navigation Window**, right-click the NE to view the shortcut menu, point to **NE**, then click **Edit In-Service (IS from OOS_MA)**. A **Confirmation** dialog box displays asking if you are sure you want to place the facility in-service.

__ 2. Click **OK**. An Information box displays confirming that the NE is in-service.

__ 3. Click **OK**.

Provisioning an NE Out-of-Service

7.07 Place an NE out-of-service by performing the following steps:

— 1. In the **Navigation Window**, right-click the NE to view the shortcut menu, point to **NE**, then click **Edit Out-Of-Service (OOS_MA)**. A **Confirmation** dialog box displays.

__ 2. In the **Command Mode** area, click **Forced** or **Normal**.

Note: *Click **Forced** if you want to ignore impact on traffic and suppress alarms, events and other system messages that describe the consequences of the action. Click **Normal** if you want to view alarms, events, and other system messages that describe the consequences of the action.*

__ 3. Click **OK**. An Information box displays confirming that the NE is out-of-service.

__ 4. Click **OK**.

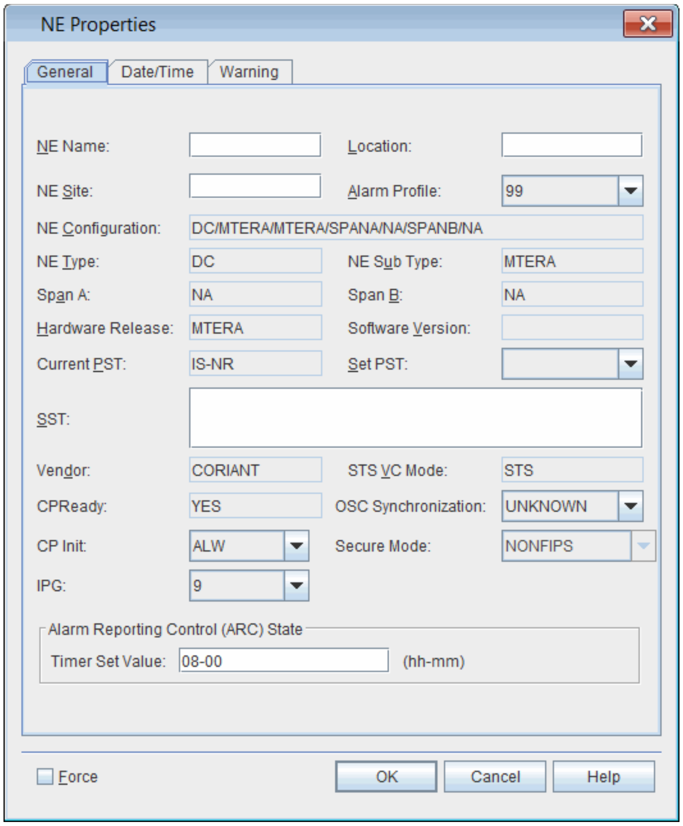
Viewing NE Properties

7.8 Review the properties of the NE by performing the following step:

__ 1. In the **Navigation Window**, right-click the **NE** icon to view the shortcut menu. Then, click **Properties**. The **NE Properties** dialog box displays. Refer to Figure 7.2, page 15-126.

7.9 Some fields in this dialog box are read-only. Refer to Table 7.2, page 15-126 for a description of the fields.

Figure 7.2 NE Properties



NE Name:

Location:

NE Site:

Alarm Profile: 99

NE Configuration: DC/MTERA/MTERA/SPANA/NA/SPANB/NA

NE Type: DC

NE Sub Type: MTERA

Span A: NA

Span B: NA

Hardware Release: MTERA

Software Version:

Current PST: IS-NR

Set PST:

SST:

Vendor: CORIANT

STS VC Mode: STS

CPReady: YES

OSC Synchronization: UNKNOWN

CP Init: ALW

Secure Mode: NONFIPS

IPG: 9

Alarm Reporting Control (ARC) State

Timer Set Value: 08-00 (hh-mm)

□ Force

Table 7.2 Fields in NE Properties Dialog Box

Field	Definition
NE Name	Name assigned to NE: up to 64 characters
NE Configuration	Current NE configuration
NE Type	This field defaults to the NE type selected in the NE Configuration box
NE Site	Name or CLLI of the site where this NE resides
Span A	NA
Hardware Release	MTERA
Current PST	Current state: IS or OOS
Location	Physical location of NE
NE Sub Type	This field defaults to the NE type selected in the NE Configuration box
Span B	NA
Software Version	Software running on processor module
Set PST	Change current state: IS or OOS
SST	Current secondary state

Table 7.2 Fields in NE Properties Dialog Box (Continued)

Field	Definition
Vendor	Coriant
STS VC Mode	Specifies whether this NE is configured for STS (SONET) or VC (SDH) mode
CP Ready	Specifies whether or not the Control Plane is ready to accept new calls or will allow configuration of new entities.
OSC Synchronization	Specifies the role of the transmitted OSC synchronization. UNKNOWN if OSC is not providing any timing or it does not matter what is happening with the OSC in regards to timing. SOURCE if OSC is acting as a Source of timing for a downstream element. When this option is selected, the system detects and reports the presence of versions of the SPM that do not support this function. THRU if OSC timing is being passed-through a 7100 Nano node. When this option is selected, the system detects and reports the presence of versions of the SPM-N that do not support this function. This option is not supported on 7100 OTS systems.
Secure Mode	Specifies whether the system security is operating in Federal Information Processing Standards (FIPS) compliance mode (NONFIPS or FIPS). This parameter is configured during basic commissioning.
CP Init	Control Plane Initialization ALW indicates that control plane on the NE has been fully initialized. INH indicated that control plane on the NE has not been initialized. PHASE1 indicates that control plane on the NE has been partially initialized. In this state, all functionality is supported by the control plane on the NE except for the signaling of calls that originated from the NE and were set up prior to NE initialization.
IPG	Specifies the default minimum transmit inter-packet gap (IPG) value (8–12, default is 9).
Timer Set Value	Alarm Reporting Control (ARC) timer for STS/VC (hh-mm). Specifies the time interval to be used in the operation of the ARC feature for all STS or VC on the NE.

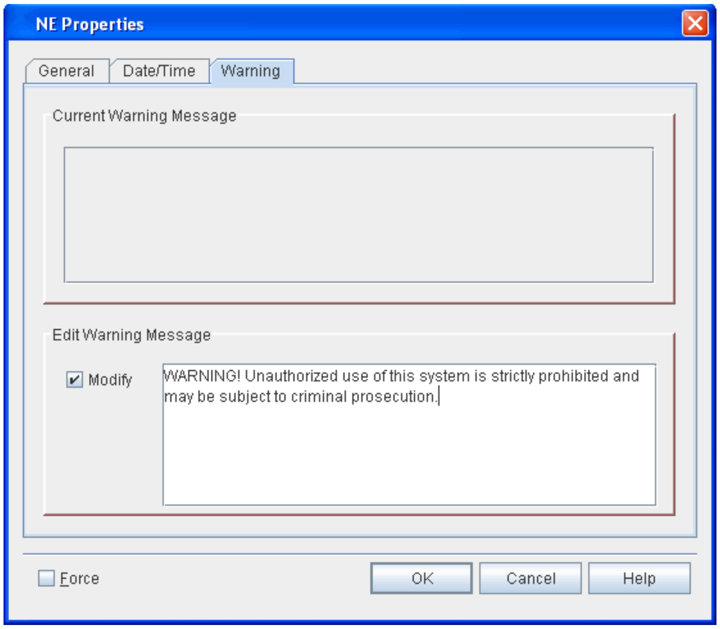
Editing NE Security Message

7.10 If company policy requires a security message prior to connecting to an NE, create and enable the security message by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NE** icon to view the shortcut menu, then click **Properties**. The **NE Properties** dialog box displays.

__ 2. Click the **Warning** tab. Refer to Figure 7.3, page 15-128.

Figure 7.3 NE Properties, Warning Tab



☑ Modify

WARNING! Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution.

□ Force

__ 3. If a warning message has been provisioned for the NE, review the text in the **Current Warning Message** area.

__ 4. If necessary, edit the warning message by performing the following steps:

__ 4.1 Click the **Modify** check box in the **Edit Warning Message** area.

__ 4.2 Type the warning message text in the box.

__ 5. Click **OK**.

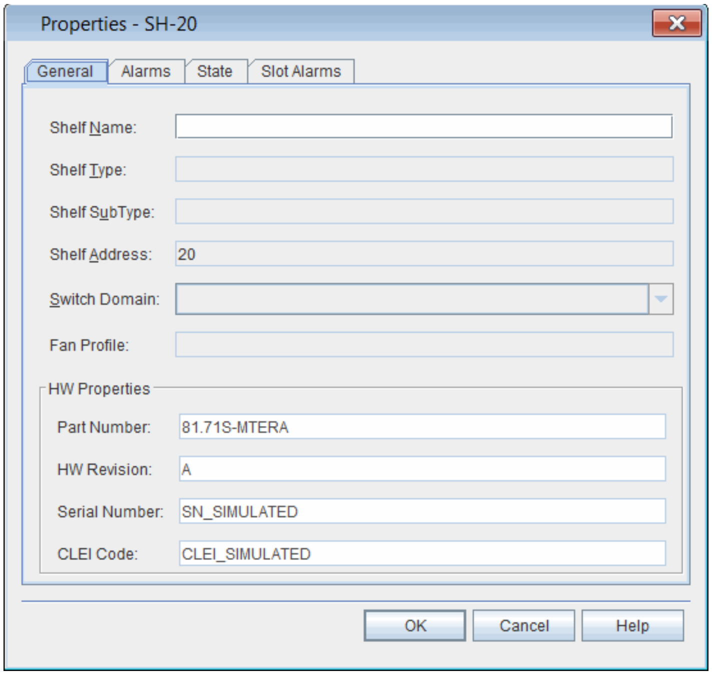
Viewing Shelf Properties

7.11 Review and modify the properties of a shelf by performing the following steps:

__ 1. In the **Navigation Window**, right-click any of the shelf icons to view the shortcut menu, then click **Properties**. The **Shelf Properties** dialog box displays.

__ 2. Click the **General** tab. Refer to Figure 7.4, page 15-129.

Figure 7.4 mTera Shelf Properties



Shelf Name:

Shelf Type:

Shelf SubType:

Shelf Address: 20

Switch Domain:

Fan Profile:

Part Number: 81.71S-MTERA

HW Revision: A

Serial Number: SN_SIMULATED

CLEI Code: CLEI_SIMULATED

__ 3. The **General** tab of the shelf **Properties** dialog box contains the following information:

- (optional) In the **Shelf Name** box, type a name for the shelf.
- The **Shelf Address** box displays the AID of the shelf.
- The following information displays in the **HW Properties** area: **Part Number**, **HW Revision**, **Serial Number**, and **CLEI Code**.

__ 4. Click the **State** tab to view the state of the shelf.

- The **Primary State** box shows the present state of the shelf.
- Click the **Secondary State** box shows the secondary state of the shelf.
- In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 5. Click the **Alarm** tab to view alarms on the shelf and the current alarm profile.

- Click the **Alarm Profile** drop-down box to change the alarm profile.

Note: *You can change the alarm profile in this screen. Refer to Defining Alarm Profiles, page 15-130 for information about defining alarm types.*

- View alarms in the **Alarm List**.

__ 6. Click the **Slot Alarms** tab to view slot alarms in the shelf.

__ 7. Click **OK**.

Modifying Shelf States

7.12 You can modify the service state of each shelf type. Right-click the **SH** icon to view the shortcut menu, point to **Shelf**, then click one of the options below:

__ **Edit Out-Of-Service** (OOS-MA): Sets the state of the shelf to out-of-service (maintenance). Click **OK** in the **Confirmation** box to continue.

__ **Edit In-Service** (IS from OOS-MA): Changes the state of the shelf from out-of-service maintenance to in-service. Click **OK** in the **Confirmation** box to continue.

__ Click **OK**.

Note: *You can also change the state of the shelf in the **Management Command** area of the shelf **Properties** dialog box.*

Defining Alarm Profiles

7.13 You can modify or assign the attributes of the alarm profile tables provided by the system for hardware, facilities, routers, or DHCP server/client entities.

7.14 The system provides 22 alarm profile tables so users can define the levels and types of alarms reported for system elements. Tables 0 and 99 are predefined and cannot be modified. Assigning Table 0 to a system element suppresses all alarms. Table 99 provides system alarm defaults. Tables 1 through 20 provide predefined sets of alarms, but the severity level of alarms other than those set as Critical can be modified.

7.15 The system defines each alarm table per entity. For example, Table 5 may be defined differently for facilities than it is for modules. Alarm severity states except for Critical can be modified. Use the alarm tables to manage and prioritize notification levels for varying condition types. Assigning different alarm profiles is also helpful when setting up or troubleshooting an NE.

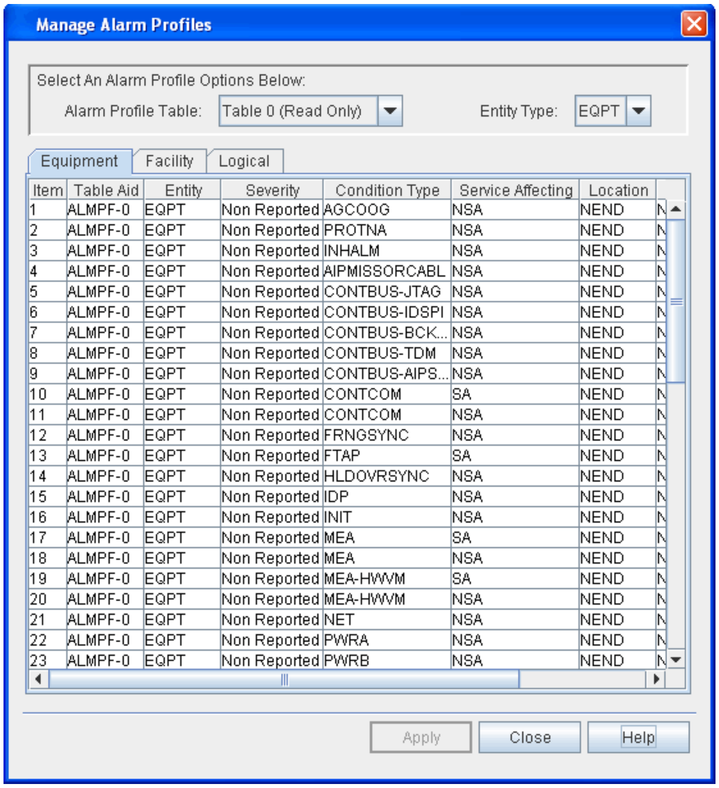
7.16 Alarm profiles can be assigned when an entity is created. If an alarm profile is not assigned, the default NE alarm profile is used. The default NE alarm profile can be 0, 1–20, or 99.

Managing Alarm Profiles

7.17 Provision alarm profile tables by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NE** icon to view the shortcut menu, then click **Alarm Profile Management**. The **Manage Alarm Profiles** dialog box displays. Refer to Figure 7.5, page 15-131.

Figure 7.5 Manage Alarm Profiles



Select An Alarm Profile Options Below:

Alarm Profile Table: Table 0 (Read Only)

Entity Type: EQPT

Item	Table Aid	Entity	Severity	Condition Type	Service Affecting	Location	
1	ALMPF-0	EQPT	Non Reported	AGCOOG	NSA	NEND	N
2	ALMPF-0	EQPT	Non Reported	PROTNA	NSA	NEND	N
3	ALMPF-0	EQPT	Non Reported	INHALM	NSA	NEND	N
4	ALMPF-0	EQPT	Non Reported	AIPMISSORCABL	NSA	NEND	N
5	ALMPF-0	EQPT	Non Reported	CONTBUS-JTAG	NSA	NEND	N
6	ALMPF-0	EQPT	Non Reported	CONTBUS-IDSPI	NSA	NEND	N
7	ALMPF-0	EQPT	Non Reported	CONTBUS-BCK...	NSA	NEND	N
8	ALMPF-0	EQPT	Non Reported	CONTBUS-TDM	NSA	NEND	N
9	ALMPF-0	EQPT	Non Reported	CONTBUS-AIPS...	NSA	NEND	N
10	ALMPF-0	EQPT	Non Reported	CONTCOM	SA	NEND	N
11	ALMPF-0	EQPT	Non Reported	CONTCOM	NSA	NEND	N
12	ALMPF-0	EQPT	Non Reported	FRNGSYNC	NSA	NEND	N
13	ALMPF-0	EQPT	Non Reported	FTAP	SA	NEND	N
14	ALMPF-0	EQPT	Non Reported	HLDOVRSYNC	NSA	NEND	N
15	ALMPF-0	EQPT	Non Reported	IDP	NSA	NEND	N
16	ALMPF-0	EQPT	Non Reported	INIT	NSA	NEND	N
17	ALMPF-0	EQPT	Non Reported	MEA	SA	NEND	N
18	ALMPF-0	EQPT	Non Reported	MEA	NSA	NEND	N
19	ALMPF-0	EQPT	Non Reported	MEA-HWVM	SA	NEND	N
20	ALMPF-0	EQPT	Non Reported	MEA-HWVM	NSA	NEND	N
21	ALMPF-0	EQPT	Non Reported	NET	NSA	NEND	N
22	ALMPF-0	EQPT	Non Reported	PWRA	NSA	NEND	N
23	ALMPF-0	EQPT	Non Reported	PWRB	NSA	NEND	N

__ 2. Click one of the three tabs: **Equipment**, **Facility**, or **Logical** to access a specific system element.

__ 3. Click the **Entity Type** drop-down box to select an entity. The type of entities that display are relevant to the tab selected. For example, if you click the **Facility** tab, go to the **Entity Type** box, and select a facility type.

__ 4. Click the **Alarm Profile Table** drop-down box to select a specific alarm table. You can modify Tables 1 through 20.

__ 5. Within the selected alarm table, locate the **Severity** column. Click any cell in this column (except where the value is Critical), and change the severity associated with that condition type.

__ 6. Click **Apply**.

Example

7.18 For example, to modify Alarm Table 3 for an OCH facility, click the **Facility** tab, click **OCH** from the **Entity Type** drop-down box, then click **Table 3** from the **Alarm Profile Table** drop-down box. Locate condition type **FDI-O** and change the severity from **Non-Reported** to **Minor**. Click **Apply**.

Implementing

7.19 Using the example above, in the **Navigation Window**, right-click the impacted **OCH** facility to view the shortcut menu. Then, click **Properties**. Click the **Alarms** tab in the **Properties** dialog box. Click the **Alarm Profile** drop-down box, and scroll to **Alarm Table 3**. Click **OK**.

mTera Synchronization

7.20 ODU switching across the mTera shelf requires that all OTN switching modules have a common clock. The STPM supports a stratum-3 level clock and distributes timing through the mTera shelf.

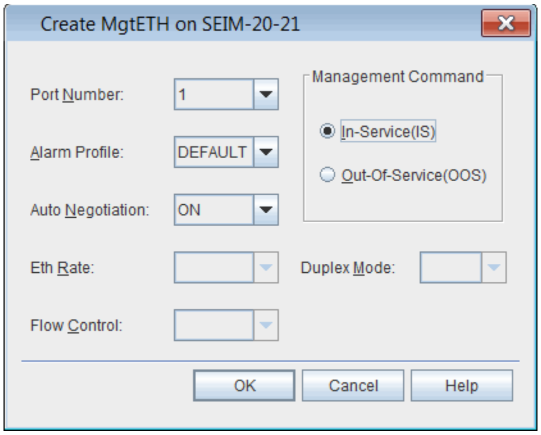
MGTETH Facility

7.21 The SEIM supports eight management Ethernet (MGTETH) facilities. The mTera automatically creates DCN MGTETH entities (MGTETH-20- [21,28]-8).

7.22 Create a MGTETH facility by performing the following steps:

__ 1. In the **Navigation Window**, right-click the SEIM to view the shortcut menu, then click **Create MgtETH Facility**. The **Create MgtETH on SEIM** dialog box displays. Refer to Figure 7.6, page 15-132.

Figure 7.6 Create MgtETH on SEIM



Create MgtETH on SEIM-20-21

Port Number: 1

Alarm Profile: DEFAULT

Auto Negotiation: ON

Eth Rate:

Duplex Mode:

Flow Control:

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

__ 2. Click the **Port Number** drop-down box to select the port number (**1**–**7**).

__ 3. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0**–**20**, **99**).

__ 4. Click the **Auto Negotiation** drop-down box to select **AUTO**, **OFF**, or **ON**. This parameter specifies if 802.3 auto-negotiation signaling is enabled (on) or disabled (off) on the management ETH facility.

__ 5. Choose one of the following options:

- If you configured Auto Negotiation to OFF, go to step 6, page 15-132.
- If you configured Auto Negotiation to AUTO or ON, go to step 9, page 15-133.

__ 6. Click the **Eth Rate** drop-down box to configure the Ethernet rate (**10**, **100**, **1000**,**10G**, **AUTO**).

__ 7. Click the **Duplex Mode** drop-down box to configure the duplex mode (**FDPLEX**, **HDPLX**, or **AUTO**).

__ 8. Click the **Flow Control** drop-down box to specify the type of flow control:

- **OFF** indicates no pause frames are supported
- **TXRX** indicates symmetric (transmit and receive)
- **TX** indicates transmit direction only
- **RX** indicates receive direction only

__ 9. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

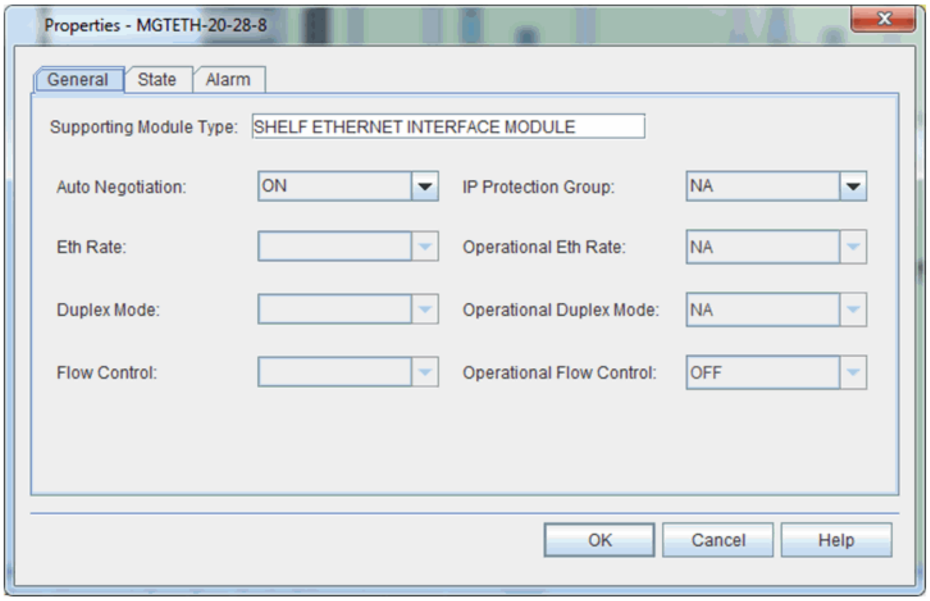
__ 10. Click **OK**.

Modifying MGTETH Facility

7.23 View or modify the properties of a MGTETH facility by performing the following steps:

__ 1. In the **Navigation Window**, right-click the MGTETH to view the shortcut menu, then click **Properties**. The **Properties - MGTETH** dialog box displays. Refer to Figure 7.7, page 15-133.

Figure 7.7 Properties - MGTETH



Supporting Module Type: SHELF ETHERNET INTERFACE MODULE

Auto Negotiation: ON

IP Protection Group: NA

Eth Rate:

Operational Eth Rate: NA

Duplex Mode:

Operational Duplex Mode: NA

Flow Control:

Operational Flow Control: OFF

__ 2. Click the **Auto Negotiation** drop-down box to select AUTO, OFF, or ON. This parameter specifies if 802.3 auto-negotiation signaling is enabled (on) or disabled (off) on the management ETH facility.

__ 3. Choose one of the following options:

- If you configured Auto Negotiation to OFF, go to step 4, page 15-134.
- If you configured Auto Negotiation to AUTO or ON, go to step 8, page 15-134.

__ 4. Click the **Eth Rate** drop-down box to configure the Ethernet rate (**10**, **100**, **1000**,**10G**, **AUTO**).

__ 5. Click the **Duplex Mode** drop-down box to configure the duplex mode (**FDPLEX**, **HDPLX**, or **AUTO**).

__ 6. Click the **Flow Control** drop-down box to specify the type of flow control:

- **OFF** indicates no pause frames are supported
- **TXRX** indicates symmetric (transmit and receive)
- **TX** indicates transmit direction only
- **RX** indicates receive direction only

__ 7. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 8. Click **OK**.

8. Managing System Performance

8.1 This section describes managing optical power settings, performance data, and loopbacks.

8.2 You can measure optical power per wavelength and direction, and then the Craft Station displays the results in tables.

8.3 System performance data is collected at regular time intervals and stored in registers for eventual output to a report.

8.4 Set loopbacks on port module facilities to test signal transmission.

Note: *Refer to TL1 Command Reference Manual for additional details on system performance parameters. Click the Help menu in the Craft Station to access this document.*

Setting Up Performance Monitoring

8.5 The Craft Station collects and monitors performance data on specific facilities on the NE. When you enable performance monitoring, the Craft Station collects specific performance parameters at regular time intervals and then stores the data in registers for eventual output to a report. Access the common performance monitoring menu by right-clicking the selected entity in the Navigation Window.

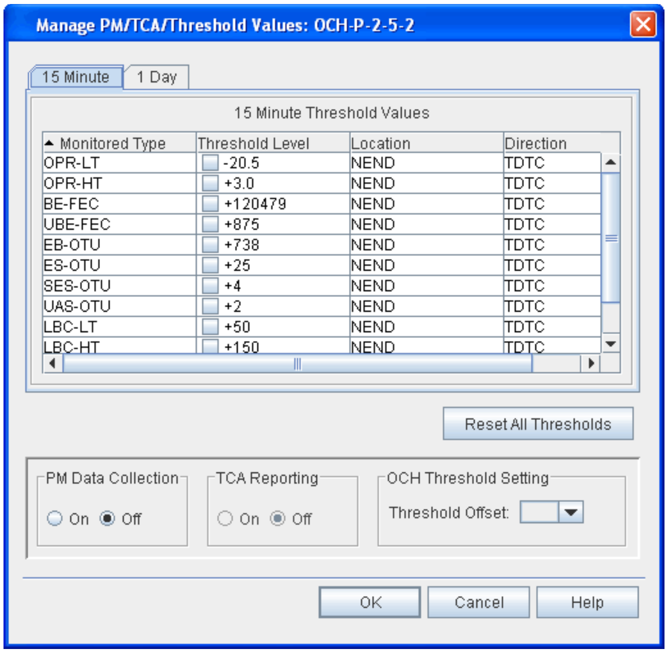
Provisioning PM on Facilities

8.06 Provision performance monitoring parameters on facilities by performing the following steps:

__ 1. Navigate to the selected entity in the **Navigation Window**.

__ 2. Right-click the entity to view the shortcut menu, then click **Manage PM Point**. The **Manage PM/TCA/Threshold Values** dialog box displays. Refer to Figure 8.1, page 15-136.

Figure 8.1 Manage PM/TCA/Threshold Values (Facility)



Manage PM/TCA/Threshold Values: OCH-P-2-5-2

15 Minute | 1 Day

15 Minute Threshold Values

Monitored Type	Threshold Level	Location	Direction
OPR-LT	□ -20.5	NEND	TDTC
OPR-HT	□ +3.0	NEND	TDTC
BE-FEC	□ +120479	NEND	TDTC
UBE-FEC	□ +875	NEND	TDTC
EB-OTU	□ +738	NEND	TDTC
ES-OTU	□ +25	NEND	TDTC
SES-OTU	□ +4	NEND	TDTC
UAS-OTU	□ +2	NEND	TDTC
LBC-LT	□ +50	NEND	TDTC
LBC-HT	□ +150	NEND	TDTC

Reset All Thresholds

PM Data Collection: ○ On ● Off

TCA Reporting: ○ On ● Off

OCH Threshold Setting: Threshold Offset:

OK Cancel Help

__ 3. If necessary, click the **Threshold Level** check box for 15 Minute Threshold Values or 1 Day Threshold Values to change the threshold level.

__ 4. If necessary, click **On** or **Off** in the **PM Data Collection** area to turn PM data collection on or off.

__ 5. If necessary, click **On** or **Off** in the **TCA Reporting** area to turn TCA reporting on or off.

__ 6. If necessary, reset data thresholds to their default values by performing one of the following steps:

- To reset an individual register, click the check box in the **Threshold Level** column. The value changes to **DFLT**.

or

- To reset all registers, click **Reset All Thresholds**.

__ 7. In the **OCH Threshold Setting** area, click the **Threshold Offset** drop-down box to select the OCH threshold Offset (**0.0–6.0**).

__ 8. Click **OK**.

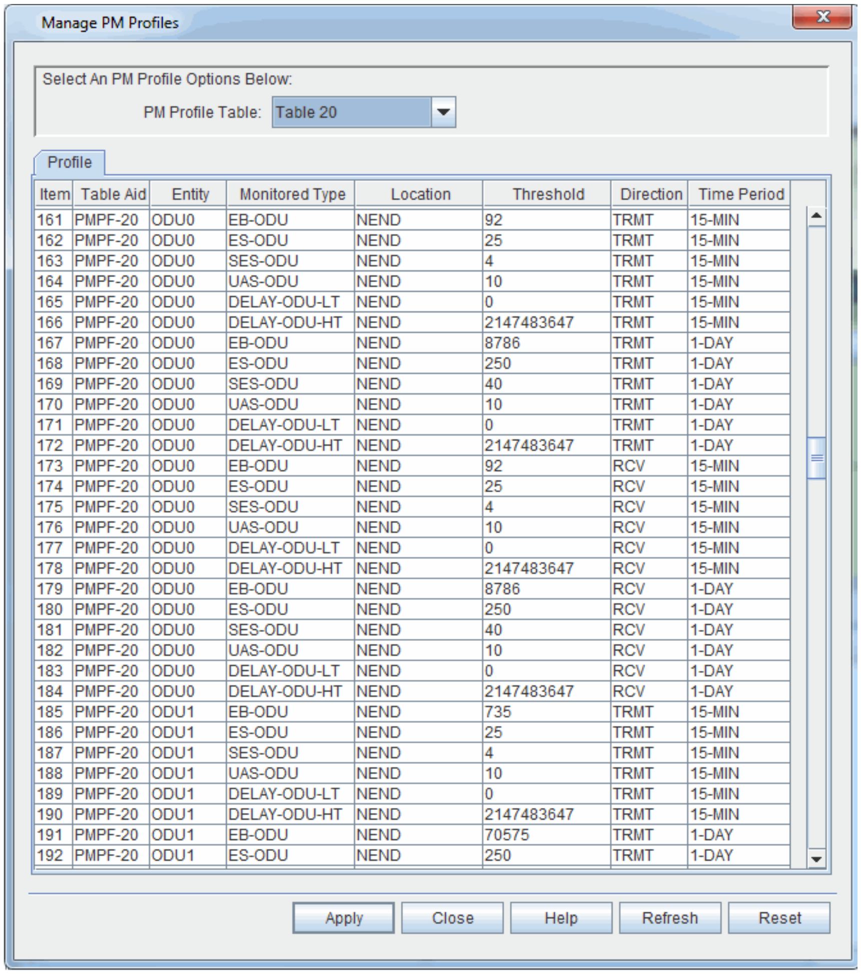
Note: *You can also turn on performance monitoring when facilities and cross-connects are provisioned.*

Managing Performance Monitoring Profile

8.7 The NE uses PM profiles on ODUk and MGTETH facilities, for which a violation triggers a TCA. Retrieve performance monitoring profiles by performing the following steps:

__ 1. In the **Navigation Window**, right-click an NE to view the shortcut menu, then click **PM Profile Management**. The **PM Profile Management** dialog box displays. Refer to Figure 8.2, page 15-137.

Figure 8.2 Manage PM Profiles



PM Profile Table: Table 20

Item	Table Aid	Entity	Monitored Type	Location	Threshold	Direction	Time Period
161	PMPF-20	ODU0	EB-ODU	NEND	92	TRMT	15-MIN
162	PMPF-20	ODU0	ES-ODU	NEND	25	TRMT	15-MIN
163	PMPF-20	ODU0	SES-ODU	NEND	4	TRMT	15-MIN
164	PMPF-20	ODU0	UAS-ODU	NEND	10	TRMT	15-MIN
165	PMPF-20	ODU0	DELAY-ODU-LT	NEND	0	TRMT	15-MIN
166	PMPF-20	ODU0	DELAY-ODU-HT	NEND	2147483647	TRMT	15-MIN
167	PMPF-20	ODU0	EB-ODU	NEND	8786	TRMT	1-DAY
168	PMPF-20	ODU0	ES-ODU	NEND	250	TRMT	1-DAY
169	PMPF-20	ODU0	SES-ODU	NEND	40	TRMT	1-DAY
170	PMPF-20	ODU0	UAS-ODU	NEND	10	TRMT	1-DAY
171	PMPF-20	ODU0	DELAY-ODU-LT	NEND	0	TRMT	1-DAY
172	PMPF-20	ODU0	DELAY-ODU-HT	NEND	2147483647	TRMT	1-DAY
173	PMPF-20	ODU0	EB-ODU	NEND	92	RCV	15-MIN
174	PMPF-20	ODU0	ES-ODU	NEND	25	RCV	15-MIN
175	PMPF-20	ODU0	SES-ODU	NEND	4	RCV	15-MIN
176	PMPF-20	ODU0	UAS-ODU	NEND	10	RCV	15-MIN
177	PMPF-20	ODU0	DELAY-ODU-LT	NEND	0	RCV	15-MIN
178	PMPF-20	ODU0	DELAY-ODU-HT	NEND	2147483647	RCV	15-MIN
179	PMPF-20	ODU0	EB-ODU	NEND	8786	RCV	1-DAY
180	PMPF-20	ODU0	ES-ODU	NEND	250	RCV	1-DAY
181	PMPF-20	ODU0	SES-ODU	NEND	40	RCV	1-DAY
182	PMPF-20	ODU0	UAS-ODU	NEND	10	RCV	1-DAY
183	PMPF-20	ODU0	DELAY-ODU-LT	NEND	0	RCV	1-DAY
184	PMPF-20	ODU0	DELAY-ODU-HT	NEND	2147483647	RCV	1-DAY
185	PMPF-20	ODU1	EB-ODU	NEND	735	TRMT	15-MIN
186	PMPF-20	ODU1	ES-ODU	NEND	25	TRMT	15-MIN
187	PMPF-20	ODU1	SES-ODU	NEND	4	TRMT	15-MIN
188	PMPF-20	ODU1	UAS-ODU	NEND	10	TRMT	15-MIN
189	PMPF-20	ODU1	DELAY-ODU-LT	NEND	0	TRMT	15-MIN
190	PMPF-20	ODU1	DELAY-ODU-HT	NEND	2147483647	TRMT	15-MIN
191	PMPF-20	ODU1	EB-ODU	NEND	70575	TRMT	1-DAY
192	PMPF-20	ODU1	ES-ODU	NEND	250	TRMT	1-DAY

__ 2. Click the **PM Profile Table** drop-down box to select the PM profile table (**Table 0**, **Table 1**–**Table 20**, **Table 99**). Table 0 and Table 99 are read-only.

__ 3. In the **Profile** tab, click to highlight a target row.

__ 4. In the **Threshold** column, type the new threshold level.

__ 5. Click **Apply**. An **Information** box displays.

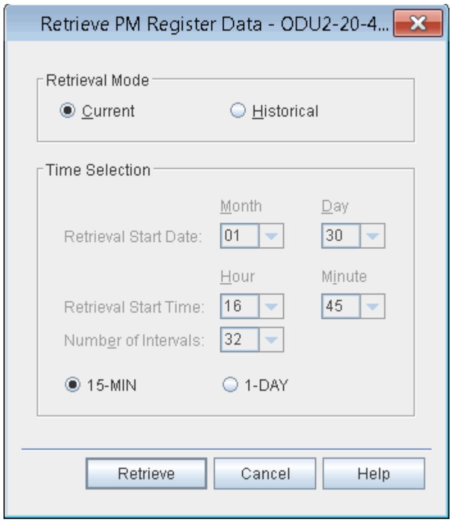
__ 6. Click **OK**.

Retrieving Performance Monitoring Data

8.8 Retrieve performance data by performing the following steps. You can specify parameters (for example, current or historical data) to filter the performance monitoring data that is collected. The example in this procedure uses the ODU2 as the target facility.

__ 1. In the **Navigation Window**, right-click the target module or facility to view the shortcut menu, point to **Performance Monitoring**, then click **View PM Point**. The **Retrieve PM Register Data** dialog box displays. Refer to Figure 8.3, page 15-138.

Figure 8.3 Retrieve PM Register Data



Retrieve PM Register Data - ODU2-20-4...

Retrieval Mode

● Current ○ Historical

Time Selection

Retrieval Start Date: Month 01 Day 30

Retrieval Start Time: Hour 16 Minute 45

Number of Intervals: 32

● 15-MIN ○ 1-DAY

__ 2. In the **Retrieve PM Register Data** dialog box, define the parameters for data collection using the following fields:

__ **Retrieval Mode**: **Current** or **Historical**

__ Click **Current** to retrieve current collected performance data. If you click **15-MIN** for the interval, a snapshot of the data collected thus far into the current quarter hour displays. If you click **1-DAY** for the interval, a snapshot of the data for the last 24 hours (or the data collected thus far into the 24-hour period) displays. Collection starts when you click the **Retrieve** button.

__ Click **Historical** to collect data stored in registers from a specific **Date** and **Time**. Go to the **Time Selection** area to set the date and time parameters. The default settings for these time parameters allow you to retrieve all available historical PM for the selected entity by clicking **Retrieve**. If you select collection for 15-minute intervals, enter the date and time (hour and minutes) for which you want data retrieved. If you select collection for 1-day intervals, the system retrieves data for the 24-hour period prior to the date (month/day) entered. You can also select the **Number of Intervals** to collect performance data.

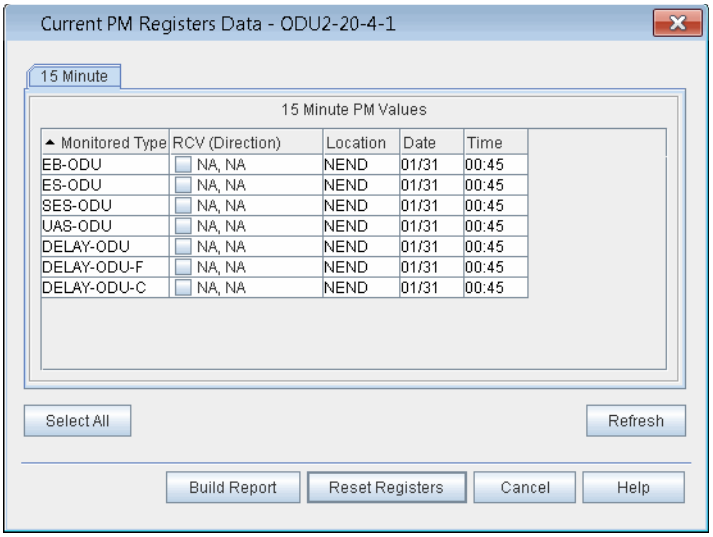
Note: *Specify an interval value of 1 to 32 for 15-minute performance monitoring registers or 1 to 7 for 1-day performance monitoring registers.*

- __ **15-MIN** or **1-DAY**: Frequency with which to retrieve performance data: each 15-minute period or each 24-hour period.

Note: *Set the **Configure PM** state of the facility to ON to capture these values. Refer to Setting Up Performance Monitoring, page 15-135 for details on how to set the state to ON. If the state is set to OFF, a warning line at the bottom of the dialog box indicates the facility is currently off, meaning performance collection cannot begin.*

__ 3. Click **Retrieve**, and the collected data displays in a table. Refer to Figure 8.4, page 15-139.

Figure 8.4 Retrieve PM Registers Data



▲ Monitored Type	RCV (Direction)	Location	Date	Time
EB-ODU	□ NA, NA	NEND	01/31	00:45
ES-ODU	□ NA, NA	NEND	01/31	00:45
SES-ODU	□ NA, NA	NEND	01/31	00:45
UAS-ODU	□ NA, NA	NEND	01/31	00:45
DELAY-ODU	□ NA, NA	NEND	01/31	00:45
DELAY-ODU-F	□ NA, NA	NEND	01/31	00:45
DELAY-ODU-C	□ NA, NA	NEND	01/31	00:45

__ 4. (Optional) Click **Reset Registers** to reset a PM register.

__ 5. Click **Build Report**, and a performance data report displays.

__ 6. Click the **File** menu to save, export, or print the report.

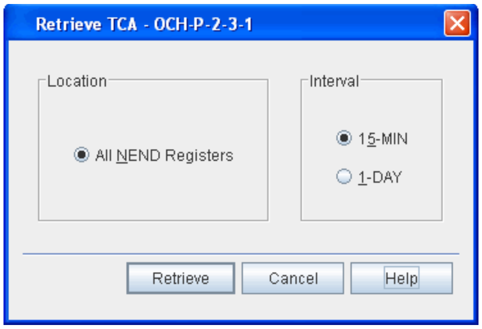
- When exporting the data as html or txt, change the encoding setting to **UTF-8** in the **Export** dialog box so the data exports correctly and your internet browser recognizes the file.
- When exporting the data as plain text file, confirm the settings for **Font spacing** in the **Export** dialog box are 12 cpi and 10 lpi for easier to read text.

Retrieving Threshold Crossing Alerts

8.9 Retrieve the data collected on system operations that crossed defined threshold values by performing the following steps:

__ 1. In the **Navigation Window**, right-click the selected module or facility to view the shortcut menu, point to **Performance Monitoring**, then click **View TCA**. The **Retrieve TCA** dialog box displays. Refer to Figure 8.5, page 15-140.

Figure 8.5 Retrieve TCA



Retrieve TCA - OCH-P-2-3-1

Location

● All NEND Registers

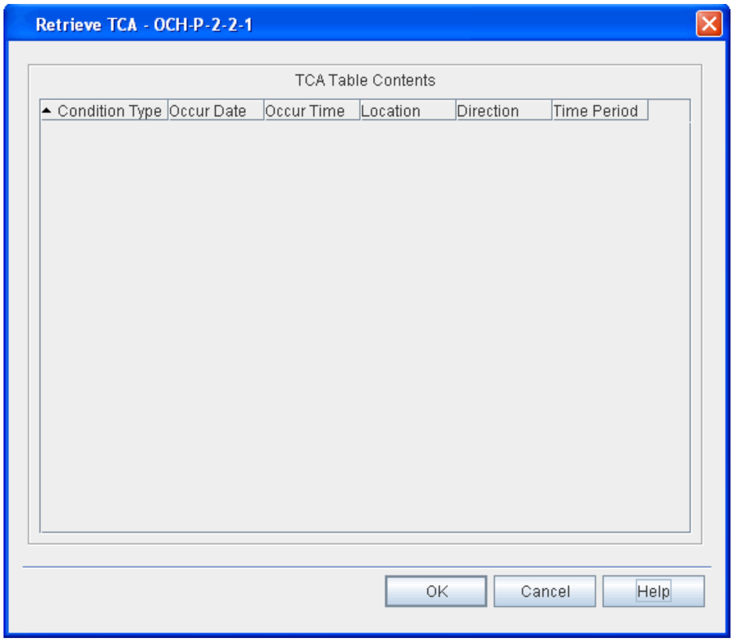
Interval

● 15-MIN

○ 1-DAY

__ 2. Select the collection **Location** and **Interval**. The entity type determines the location options. Select the time interval: **15-MIN** or **1-Day**. Click **Retrieve**, and a dialog box showing the TCA values displays. Refer to Figure 8.6, page 15-140 for an example.

Figure 8.6 Retrieve TCA for OCH-P



Retrieve TCA - OCH-P-2-2-1

TCA Table Contents

Condition Type	Occur Date	Occur Time	Location	Direction	Time Period

Managing Performance Reports

8.10 As the Craft Station monitors the performance of an NE, you can organize the data into reports for troubleshooting purposes. You can schedule these reports for delivery at specific intervals. Or, you can define and save the parameters and delivery schedule of the report until the report is requested.

Note: *Use the 7194 Network Management System to capture performance data for an entire circuit supported by multiple NEs.*

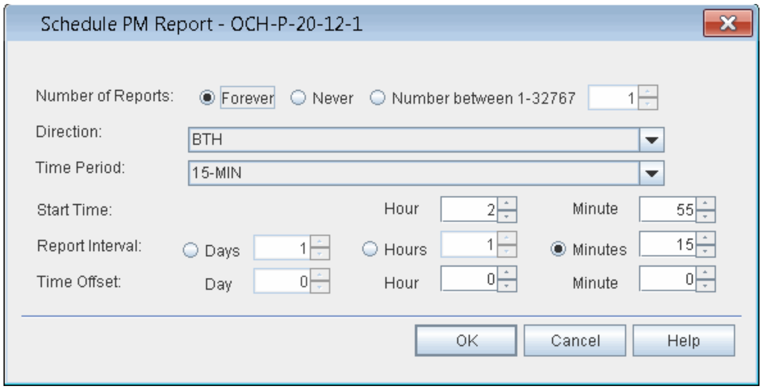
8.11 Collect and use historical data to isolate system problems by tracking performance during system start-up, after power re-baselines, and by tracing threshold crossing events.

Scheduling PM Reports

8.12 Set up and initiate performance reports by performing the following steps:

__ 1. In the **Navigation Window**, right-click the selected entity to view the shortcut menu, point to **Performance Monitoring**, point to **Manage PM Report**, then click **Schedule PM Report**. Refer to Figure 8.7, page 15-141. Use this dialog box to define the time parameters for scheduling the report. Enter values for the following fields:

Figure 8.7 Schedule PM Report



Schedule PM Report - OCH-P-20-12-1

Number of Reports: ● Forever ○ Never ○ Number between 1-32767 1

Direction: BTH

Time Period: 15-MIN

Start Time: Hour 2 Minute 55

Report Interval: ○ Days 1 ○ Hours 1 ● Minutes 15

Time Offset: Day 0 Hour 0 Minute 0

- **Number of Reports**: The number of times the system generates a report. Select **Forever** to run a report continuously at the scheduled time. Select **Never** to cancel PM reports. Specify a **Number between 1–32767** to run a report for a specific number of intervals.
- **Direction**: Network direction of the measurement. **BTH** for both directions, **TDTC** for transmit direction toward customer, **TDTN** for transmit direction toward network, or **NA** for not applicable (no direction).
- **Start Time**: Hour and Minute when performance data collection starts.
- **Report Interval**: Defines how frequently the report runs in **Days**, **Hours**, or **Minutes**.
- **Time Offset**: Time-period increments during which PM data collects: **Days**, **Hours**, or **Minutes**.

__ 2. Click **OK**.

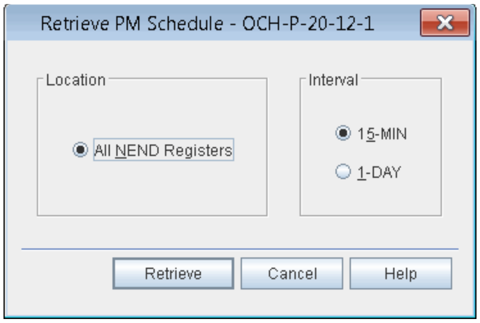
__ 3. Click **OK** in the **Confirmation** box.

Retrieving PM Schedule

__ 4. In the **Navigation Window**, right-click the selected entity to view the shortcut menu, point to **Performance Monitoring**, point to **Manage PM Report**, then click **Retrieve PM Schedule**. Refer to Figure 8.8, page 15-142. Use this dialog box to define the parameters for retrieving a report. Enter values for the following fields:

- **Location**: retrieve schedule for this network location.
- **Interval**: retrieve schedule for this pre-defined duration.

Figure 8.8 Retrieve PM Schedule



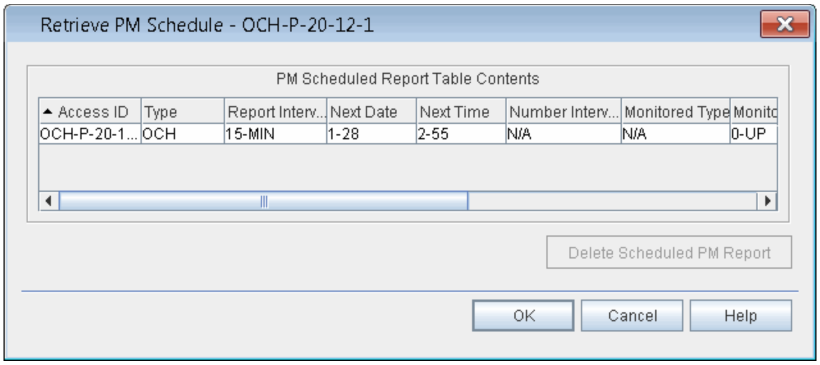
Retrieve PM Schedule - OCH-P-20-12-1

Location: ● All NEND Registers

Interval: ● 15-MIN ○ 1-DAY

__ 5. Click **Retrieve** to review the schedule. Refer to Figure 8.9, page 15-142.

Figure 8.9 Retrieve PM Schedule



Retrieve PM Schedule - OCH-P-20-12-1

PM Scheduled Report Table Contents

Access ID	Type	Report Interv...	Next Date	Next Time	Number Interv...	Monitored Type	Monitc
OCH-P-20-1...	OCH	15-MIN	1-28	2-55	N/A	N/A	0-UP

Deleting Scheduled PM Report

__ 6. If necessary, delete a scheduled PM report by performing the following substeps:

__ 6.1 Click to highlight the scheduled PM report in the **PM Scheduled Report Table Contents** area.

__ 6.2 Click **Delete Scheduled PM Report**.

__ 6.3 Click **OK**.

Allowing PM Report

__ 7. In the **Navigation Window**, right-click the entity to view the shortcut menu, point to **Performance Monitoring**, point to **Manage PM Report**, then click **Allow PM Reports**. A **Confirmation** box displays.

__ 8. Click **OK** to allow PM reports.

Inhibiting PM Report

__ 9. In the **Navigation Window**, right-click the entity to view the shortcut menu, point to **Performance Monitoring**, point to **Manage PM Report**, then click **Inhibit PM Reports**. A **Confirmation** box displays.

> ***Note:*** *Avoid the unnecessary collection of data during periods such as when equipment is being replaced by inhibiting PM reports. Report collection settings are saved for when reporting is allowed.*

__ 10. Click **OK** to inhibit PM reports.

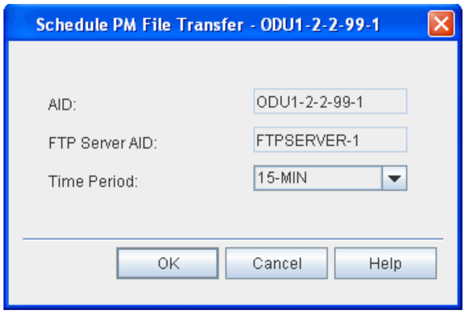
Managing PM File

8.13 Use an FTP server to export performance monitoring reports on ODU or MGTETH entities. Information on setting up an FTP server to retrieve or export facility performance monitoring data can be found in Creating an FTP Server, page 15-122.

8.14 Set up PM on a facility by performing the following steps:

__ 1. In the **Navigation Window**, right-click the selected entity to view the shortcut menu, point to **Performance Monitoring**, point to **PM File**, then click **Schedule**. The **Schedule PM File Transfer** dialog box displays. Refer to Figure 8.10, page 15-143.

Figure 8.10 Schedule PM File Transfer



Schedule PM File Transfer - ODU1-2-2-99-1

AID: ODU1-2-2-99-1

FTP Server AID: FTPSERVER-1

Time Period: 15-MIN

- The **AID** box lists the AID of the target entity for PM data collection.
- The **FTP Server AID** box contains the AID of the FTP server.

__ 2. Click the **Time Period** drop-down box to select **15-MIN** or **1-DAY**.

__ 3. Click **OK**. An **Information** box displays indicating that the PM file transfer was successfully scheduled.

8.15 Follow local procedures to retrieve the PM file from the FTP server.

Testing Transmission Integrity

8.16 The diagnostic features described in this section test the integrity of the transponder transmission spans. One test verifies that the forward error correction (FEC) feature is working by transmitting one or more correctable FEC block errors on the line side of a transponder to test correction function at the far-end. Under normal conditions, a review of incrementing Blocked Error Forward Error Correction (BE-FEC) performance data on the OCH-P of the remote transponder confirms that the FEC function is working normally. The system supports this feature on the following facilities:

- OCH-P facility supported by OSM-2S (when FEC type is set to regular)
- OTU2 supported by OSM-2S

8.17 Set the associated facility **FEC** parameter to **Regular** or **Super** and set the state of the facility to IS.

Caution:

During the FEC test, keep the facility in the IS state. Moving the facility to the OOS state will affect traffic.

8.18 Since you can provision the OCH-P facility on the DWDM-side of a transponder for either Regular FEC or Super FEC, provision the transponder at each end of the lightpath for the same type of FEC. If one transponder is provisioned for Regular FEC and the other one is provisioned for Enhanced FEC, the system declares a FEC-M (FEC-Mismatch) alarm.

Note: *Confirm there are no errors on the lightpath before initiating this command. If this diagnostic runs when there are already-corrected FEC block errors on the lightpath, uncorrected errors (UBE-FEC) may result, which could skew the response and impact service.*

8.19 A second test detects failures via facility or terminal loopbacks by initiating the transmission of a Pseudo Random Binary Sequence (PRBS) pattern on the line-side or port-side of a transponder. The following facilities support PRBS:

- HGE, ODUF, ODU0, ODU1, ODU2, OC192, OTU2, OTU4, STM64, TGLAN, and OCH-P supported by OSM-2C and OSM-2s

8.20 Set the facility to out-of-service before initiating the PRBS diagnostic.

8.21 When the PRBS transmission is complete, the system reports the results. Information captured includes the following: time elapsed since PRBS was started, the reference bit error rate, number of reported errors during the collection period, and whether the PRBS pattern is synchronized. Synchronization indicates that the PRBS transmitter pattern and receiver pattern are the same. Only errors counted when PRBS is synchronized have value. If PRBS is out of synchronization, the transmitter pattern does not match the receiver pattern and, as a result, the received errors and associated error rate reflect noise.

Note 1: *Once diagnostic FEC starts, transmit PRBS is not available. Once diagnostic FEC starts, you must connect to the far-end transponder, and monitor PM to observe the correctable BE-FEC counter and confirm it is accumulating.*

Note 2: *Refer to TL1 Command Reference Manual for additional details on the PRBS transmission feature. Click the Help menu in the Craft Station to access this document.*

8.22 For modules that support the enabling/disabling of a test signal at an ODU level (OSM-2C and OSM-2S), if the client facility supported by the ODU under test has a defect, the system will transmit client signal fail-optical payload unit (CSF-OPU) to the far end during the PRBS test. The far end will detect the CSF-OPU and post a condition. (By default this condition is not alarmed.)

Starting Forward Error Correction (FEC) Diagnostics

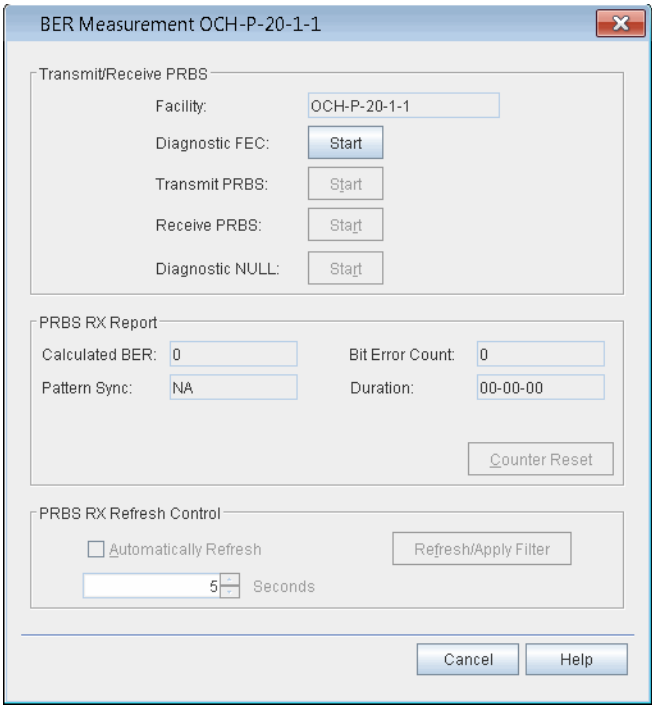
8.23 Before starting FEC diagnostics, first verify that zero BE-FEC or UBE-FEC are being received at the far end first. When you enable FEC diagnostics, the system inserts small amounts of BE-FEC towards the far end. The transponder at the far end corrects these errors and no traffic disruption occurs. Small incrementing counts of BE-FEC display at the terminating transponder OCH-P PM point. This indicates that FEC is working and the test is successful.

8.24 Start FEC diagnostics by performing the following steps:

__ 1. Navigate to the selected OCH-P in the **Navigation Window**.

__ 2. Right-click the OCH-P to view the shortcut menu, then click **BER Measurement**. The **BER Measurement** dialog box displays. Refer to Figure 8.11, page 15-146.

Figure 8.11 BER Measurement



BER Measurement OCH-P-20-1-1

Transmit/Receive PRBS

Facility: OCH-P-20-1-1

Diagnostic FEC: Start

Transmit PRBS: Start

Receive PRBS: Start

Diagnostic NULL: Start

PRBS RX Report

Calculated BER: 0

Bit Error Count: 0

Pattern Sync: NA

Duration: 00-00-00

PRBS RX Refresh Control

□ Automatically Refresh

5 Seconds

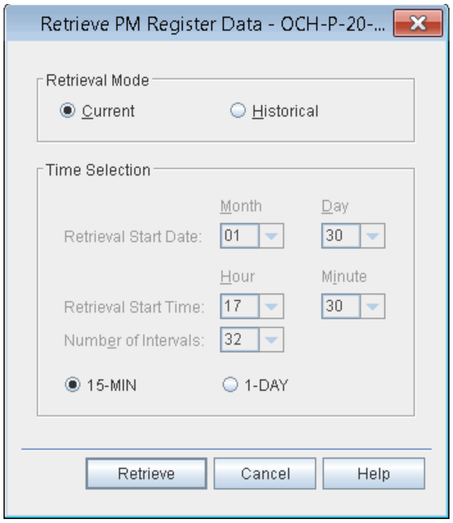
__ 3. Click the **Start** button next to **Diagnostic FEC**. A confirmation message displays, and the state of the button changes to **Stop**.

__ 4. Retrieve the BE-FEC count at the far-end transponder by performing the following steps:

__ 4.1 Start another session of the Craft Station, and connect the NE with the terminating transponder.

__ 4.2 In the **Navigation Window**, locate the far-end transponder. Click to expand the transponder. Right-click the **OCH-P** facility to view the shortcut menu, point to **Performance Monitoring**, then click **View PM Point**. The **Retrieve PM Register Data** dialog box displays. Refer to Figure 8.12, page 15-147.

Figure 8.12 Retrieve PM Register Data



Retrieve PM Register Data - OCH-P-20-...

Retrieval Mode

● Current ○ Historical

Time Selection

	Month	Day
Retrieval Start Date:	01	30

	Hour	Minute
Retrieval Start Time:	17	30
Number of Intervals:	32	

● 15-MIN ○ 1-DAY

__ 4.3 In the **Retrieval Mode** area, click **Current**.

__ 4.4 In the **Time Selection** area, click **15-MIN**.

__ 4.5 Click **Retrieve**.

__ 4.6 Monitor the performance monitoring points on the OCH-P. Note accumulations of BE-FEC errors.

Starting PRBS Diagnostics

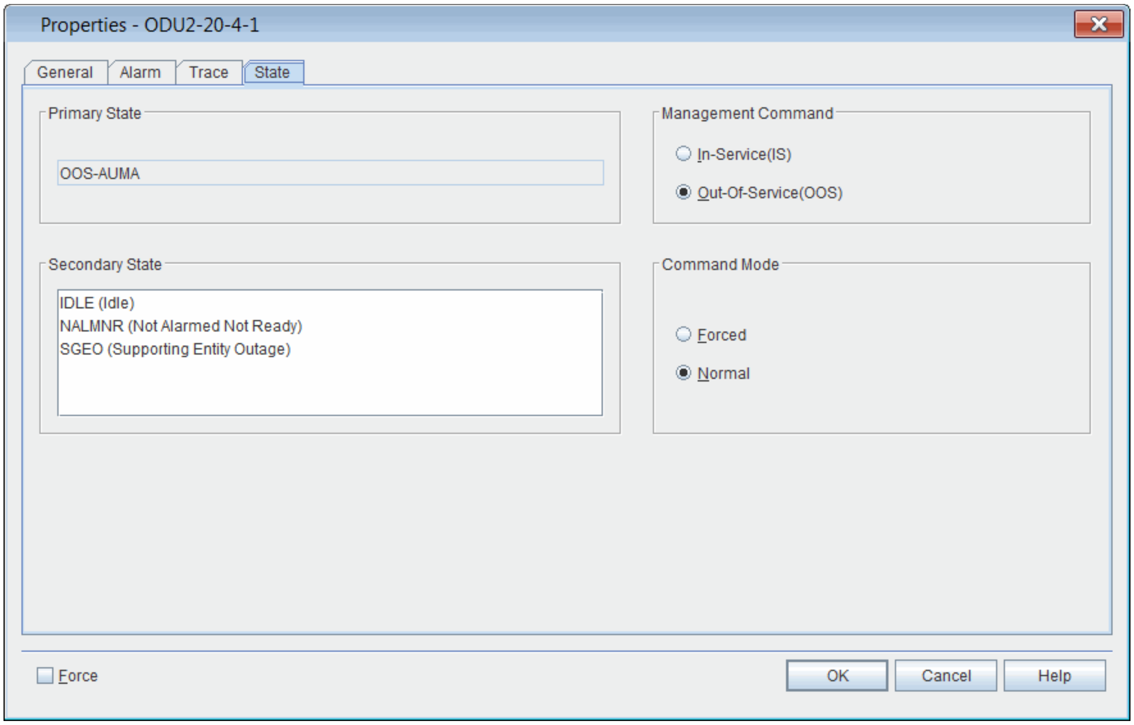
8.25 Start PRBS diagnostics by performing the following steps:

__ 1. Navigate to the selected ODUk in the **Navigation Window**.

__ 2. Right-click the ODUk to view the shortcut menu, then click **Properties**. The **Properties - OCH-P-x-x-x** dialog box displays.

__ 3. Click the **State** tab. Refer to Figure 8.13, page 15-148.

Figure 8.13 Properties - ODUk-x-x-x



Primary State: OOS-AUMA

Secondary State:
IDLE (Idle)
NALMNR (Not Alarmed Not Ready)
SGEO (Supporting Entity Outage)

Management Command:
○ In-Service(IS)
● Out-Of-Service(OOS)

Command Mode:
○ Forced
● Normal

□ Force

__ 4. Determine the state of the facility in the **Primary State** box.

__ 4.1 If the current state of the facility is out-of-service, maintenance (OOS-MA), click **Cancel**. Go to step 8, page 15-148.

__ 4.2 For all other current states, go to step 5, page 15-148.

__ 5. In the **Management Command** area, click **Out-Of-Service(OOS)**.

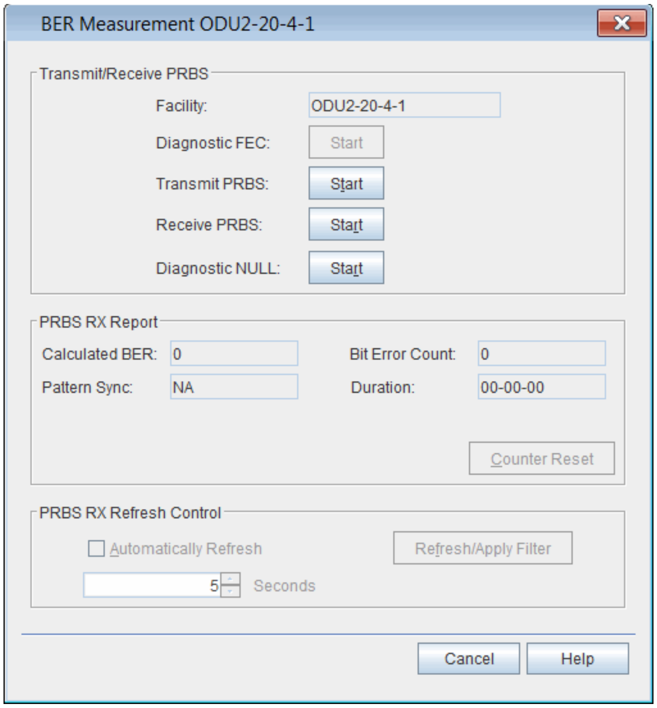
__ 6. In the **Command Mode** area, click **Forced**.

Note: *Click **Forced** if you want to ignore impact on traffic and suppress alarms, events and other system messages that describe the consequences of the action. Click **Normal** if you want to view alarms, events, and other system messages that describe the consequences of the action.*

__ 7. Click **OK**.

__ 8. In the **Navigation Window**, right-click the ODUk facility to view the shortcut menu, then click **BER Measurement**. The **BER Measurement** dialog box displays. Refer to Figure 8.14, page 15-149.

Figure 8.14 PRBS Diagnostics



Facility: ODU2-20-4-1

Diagnostic FEC: Start

Transmit PRBS: Start

Receive PRBS: Start

Diagnostic NULL: Start

Calculated BER: 0

Bit Error Count: 0

Pattern Sync: NA

Duration: 00-00-00

□ Automatically Refresh

5 Seconds

__ 9. Before starting transmit or receive PRBS, confirm one of the following conditions are met:

- __ Far-end transponder is in loopback (line facility or port terminal). Refer to Figures 8.15, page 15-151 through 8.18, page 15-152.
- __ Far-end has both transmit and receive PRBS started.

__ 10. Click the **Start** button next to **Transmit PRBS**. The state of the button changes to **Stop**, and a confirmation message displays. This step starts the transmission of the PRBS pattern.

__ 11. Click the **Start** button next to **Receive PRBS**. The state of the button changes to **Stop**, and a confirmation message displays. This step starts the capture of the PRBS diagnostics.

__ 12. The results of the transmission display in the **PRBS RX Report** box:

- The **Calculated BER** rate: A value if 5 indicates a bit error rate of 10^{-5}.
- The **Pattern Sync**: Indicates if the PRBS pattern was synchronized during testing. The testing results are valid if this field is **INSYNCH**.
- The **Bit Error Count**: The total bit error count since PRBS started.
- **Duration**: Amount of time since start of PRBS.

Note: *The PRBS duration timer only accumulates when the PRBS pattern is In-Sync (INSYNC). If the PRBS pattern is Out-of-Sync (OUTSYNC), errors do not accumulate and the PRBS duration timer does not increment.*

__ 13. Click the **Counter Reset** button to set the PRBS counters to zero and reset the timer.

Note: *The Receive PRBS button must be in the Start state before the system can reset counters.*

__ 14. Perform the following actions in the **PRBS RX Refresh Control** area:

__ Verify the **Automatically Refresh** check box is selected.

__ Use the up and down arrows to specify a time increment (in seconds) to set the receipt of PBRS to repeat at specific time periods.

__ Click **Refresh/Apply Filter** to apply the new settings to the facility that is being tested. The system polls the transponder and refreshes the results report.

__ 15. Click **OK**.

__ 16. In the **PRBS Diagnostics** dialog box, click **Stop** to end the Transmit PRBS diagnostic. Then click **Stop** to end the Receive PRBS diagnostic. Refer to Figure 8.14, page 15-149.

__ 17. Repeat steps 1, page 15-147 through 16, page 15-150 for the far-end transponder.

__ 18. If the state of the module did not change in step 5, page 15-148 the procedure is complete.

__ 19. If the state of the facility did change in step 5, page 15-148, follow the steps below to return the facility to its original state:

__ 19.1 In the **Navigation Window**, right-click the facility to view the shortcut menu, then click **Properties**. The **Properties - OCH-P-x-x-x** dialog box displays.

__ 19.2 Click the **State** tab. Refer to Figure 8.13, page 15-148.

__ 19.3 In the **Management Command** area, set the present state of the facility to the same value as in step 4, page 15-148.

__ 19.4 In the **Command Mode** area, click **Forced** or **Normal**.

Note: *Click* ***Forced*** *if you want to ignore impact on traffic and suppress alarms, events and other system messages that describe the consequences of the action. Click* ***Normal*** *if you want to view alarms, events, and other system messages that describe the consequences of the action.*

__ 19.5 Click **OK**.

__ 20. Repeat step 18, page 15-150 and step 19, page 15-150 for the far-end transponder.

Facility Loopbacks

8.26 Maintenance loopbacks cause a channel on an incoming facility to loop back on itself in the outgoing direction.

8.27 The system supports four types of loopbacks:

- facility loopback of a client signal (port side)
- facility loopback of an OCH facility (line side)
- terminal loopback of a client signal (port side)
- terminal loopback of an OCH facility (line side)

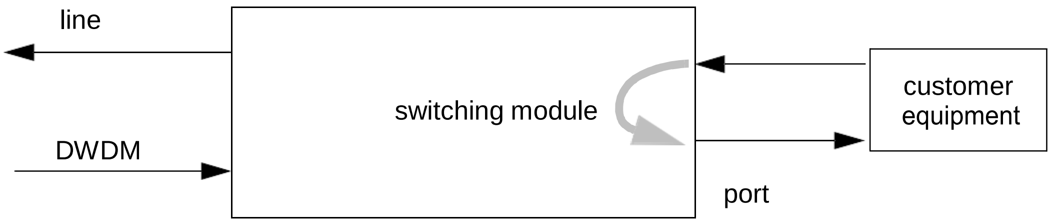
8.28 The following facilities support loopbacks: HGE, OC192, OCH-P, OTU2, OTU4, STM64, TGLAN.

Note 1: *Set the facility to out-of-service before operating a loopback.*

Note 2: *A pluggable transceiver installed in a transponder may create a power difference between the port-side transmit of the module supporting the pluggable transceiver and the port-side receive of another module in the signal path. To avoid the risk of bit errors and damage to equipment, confirm the replacement pluggable transceiver can support the reach and power level of the signal the module supports, or use an appropriate optical attenuation to bring the power in line with the receiver of the pluggable transceiver.*

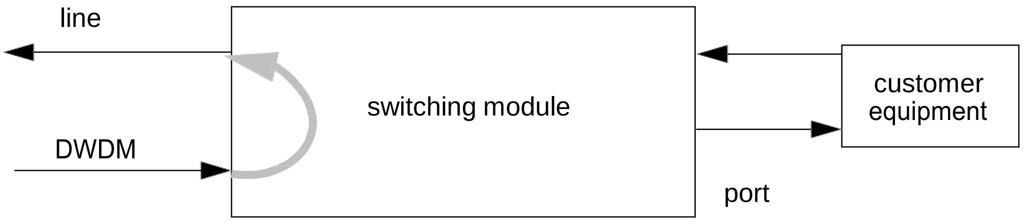
8.29 A facility loopback loops the client port-side signal back towards the customer equipment. Refer to Figure 8.15, page 15-151.

Figure 8.15 Facility Loopback of Port-Side Facility



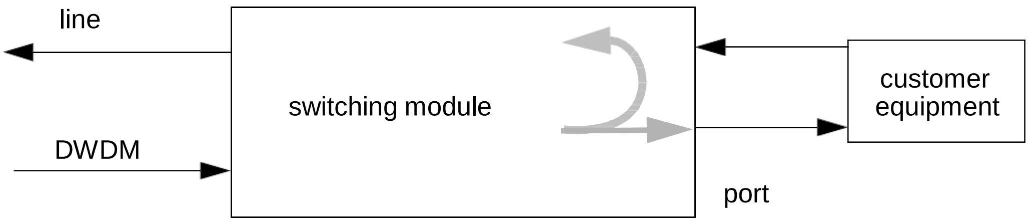
8.30 A facility loopback loops the OCH-P line-side signal back towards the DWDM network. Refer to Figure 8.16, page 15-152.

Figure 8.16 Facility Loopback of OCH-P Line-Side Facility



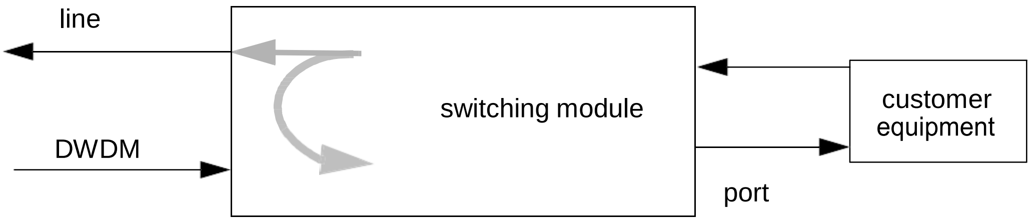
8.31 A terminal loopback loops the client port-side signal back towards the DWDM network. Refer to Figure 8.17, page 15-152.

Figure 8.17 Terminal Loopback of Port-Side Facility



8.32 A terminal loopback loops the OCH-P line-side signal back towards the customer equipment. Refer to Figure 8.18, page 15-152.

Figure 8.18 Terminal Loopback of OCH-P Line-Side Facility



Operating Loopback

8.33 Create a loopback by performing the following steps:

__ 1. In the **Navigation Window**, right-click the target facility to view the shortcut menu, point to **Operate Loopback**, then click either **Facility** or **Terminal**.

An **Information** box displays confirming the Operate Loopback action is successful and the loopback is started.

If the loopback action fails, a failed message displays, indicating the condition that blocked the loopback.

__ 2. Click **OK**.

Releasing Loopback

8.34 Release a loopback by performing the following steps:

__ 1. In the **Navigation Window**, right-click the target facility to view the shortcut menu, point to **Release Loopback**, then click either **Facility** or **Terminal**. An **Information** box displays confirming the Release Loopback action is successful and the loopback stopped.

__ 2. Click **OK**.

Measuring Optical Power

8.35 The system supports optical power measurements on the following modules: OSM-2C, and OSM-2S. The power measurement is per specific port or channel, is non-intrusive, and does not require the module to be out-of-service.

8.36 Right-click any of these modules to view the shortcut menu, then click **Measure Optical Power**. Select the signal direction, the wavelength (or channel), and its associated port (if required) to be measured, and the system retrieves the data described in Table 8.1, page 15-154. Refer to Table 8.2, page 15-154 for measurable signal directions per module.

Table 8.1 Fields for Measuring Optical Power

Field	Definition
Signal direction	Identifies the optical signal location (port, line, or express) and the signal direction (transmit or receive) of channel under test. Refer to Table 8.2, page 15-154.
Port Number	The port number (if there is more than one) associated with the signal under measurement on the port side of the module: **1 to 20** for OSM-2S **1 to 2** for OSM-2C **All**

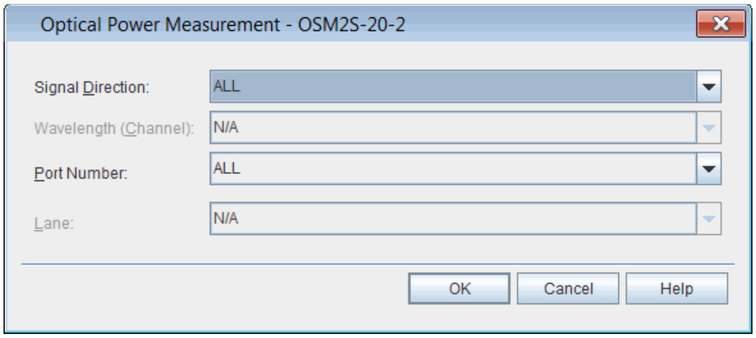
Table 8.2 Signal Direction Under Measurement

Module	Signal Direction
OSM-2C, OSM-2S	LSR - Line-Side Receive
OSM-2C, OSM-2S	LST - Line-Side Transmit
OSM-2C, OSM-2S	PSR - Port-Side Receive
OSM-2C, OSM-2S	PST - Port-Side Transmit
A value of All returns all valid measurements for that module.	

8.37 Measure optical power on relevant entities by performing the following steps:

__ 1. Right-click the module or facility to view the shortcut menu, then click **Measure Optical Power**. The **Optical Power Measurement** dialog box displays. Refer to Figure 8.19, page 15-154.

Figure 8.19 Optical Power Measurement



Optical Power Measurement - OSM2S-20-2

Signal Direction: ALL

Wavelength (Channel): N/A

Port Number: ALL

Lane: N/A

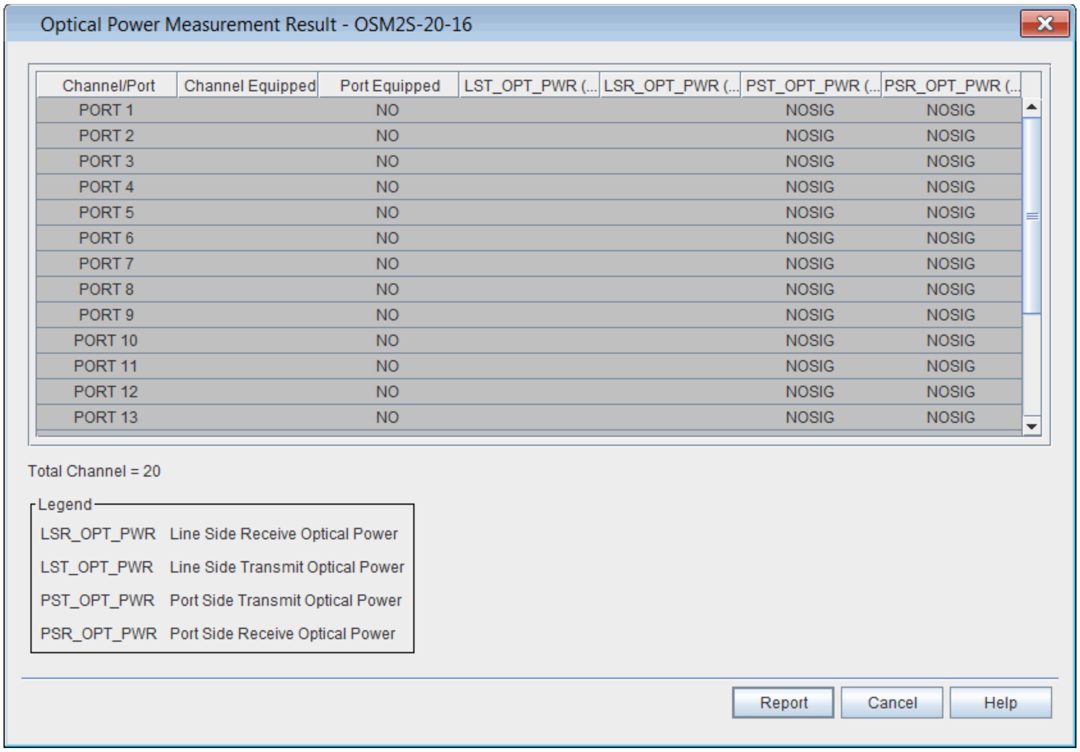
__ 2. Select the **Signal Direction** that you want to measure. Select **All** to capture all directions valid for the module/facility selected.

__ 3. Select the **Port Number**.

__ 4. Click **OK**.

8.38 The system captures the requested data and returns it formatted similarly to the window shown in Figure 8.20, page 15-155.

Figure 8.20 Optical Power Measurement Results Screen for OSM-2S



Optical Power Measurement Result - OSM2S-20-16

Channel/Port	Channel Equipped	Port Equipped	LST_OPT_PWR (...	LSR_OPT_PWR (...	PST_OPT_PWR (...	PSR_OPT_PWR (...
PORT 1		NO			NOSIG	NOSIG
PORT 2		NO			NOSIG	NOSIG
PORT 3		NO			NOSIG	NOSIG
PORT 4		NO			NOSIG	NOSIG
PORT 5		NO			NOSIG	NOSIG
PORT 6		NO			NOSIG	NOSIG
PORT 7		NO			NOSIG	NOSIG
PORT 8		NO			NOSIG	NOSIG
PORT 9		NO			NOSIG	NOSIG
PORT 10		NO			NOSIG	NOSIG
PORT 11		NO			NOSIG	NOSIG
PORT 12		NO			NOSIG	NOSIG
PORT 13		NO			NOSIG	NOSIG

Total Channel = 20

Legend

LSR_OPT_PWR	Line Side Receive Optical Power
LST_OPT_PWR	Line Side Transmit Optical Power
PST_OPT_PWR	Port Side Transmit Optical Power
PSR_OPT_PWR	Port Side Receive Optical Power

8.39 You can export or save the information provided in the results screen as a report. Click **Report** and the data displays in a format appropriate for printing or saving.

System Reports

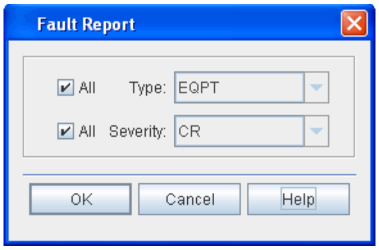
8.40 The Craft Station creates the following reports to provide information to the user: Faults, Conditions, History Alarms, DCM, VCG, EVC, Cross Connects, Facilities, Facility Protection Groups, Path Protection (ODU SCN Protection) Groups, Equipment, Fibers, Inventory, TAP, Control Plane (Call, Routing Controller Node, and Topological Link) and Software Versions. Access the reports through the Reports menu.

Faults Report

8.41 The Fault report captures all faults on the NE. Create a Fault report by performing the following steps:

__ 1. From the **Reports** menu, click **Faults**. The **Fault Report** dialog box displays. Refer to Figure 8.21, page 15-156.

Figure 8.21 Fault Report



☑ All Type: EQPT

☑ All Severity: CR

__ 2. Click **All** to select all entities, or click the **Type** drop-down box to select one entity.

__ 3. Click **All** to select all severity levels, or click the **Severity** drop-down box to select the severity level (**CR** (critical), **MJ** (major), **MN** (minor), **NA** (not alarmed), or **NR** (not reported).

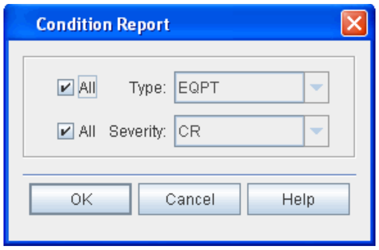
__ 4. Click **OK** to display the report.

Conditions Report

8.42 The Conditions report captures all conditions on the NE. Create a Conditions report by performing the following steps:

__ 1. From the **Reports** menu, click **Conditions**. The **Condition Report** dialog box displays. Refer to Figure 8.22, page 15-156.

Figure 8.22 Condition Report



☑ All Type: EQPT

☑ All Severity: CR

__ 2. Click **All** to select all entities, or click the **Type** drop-down box to select one entity.

__ 3. Click **All** to select all severity levels, or click the **Severity** drop-down box to select the severity level (**CR** (critical), **MJ** (major), **MN** (minor), **NA** (not alarmed), or **NR** (not reported).

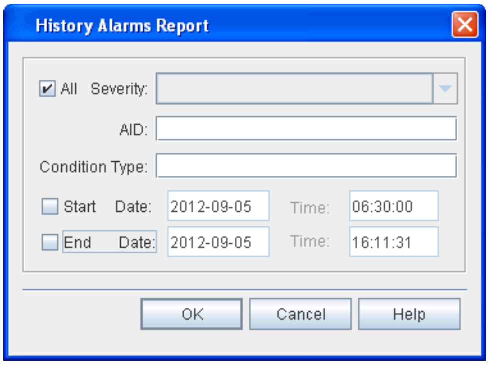
__ 4. Click **OK** to display the report.

History Alarms

8.43 Retrieve a history of the autonomous output messages stored on the NE using the History Alarms report. Create a History Alarms report by performing the following steps:

__ 1. From the **Reports** menu, click **History Alarms**. The **History Alarms Report** dialog box displays. Refer to Figure 8.23, page 15-157.

Figure 8.23 History Alarms



History Alarms Report

☑ All Severity:

AID:

Condition Type:

□ Start Date: 2012-09-05 Time: 06:30:00

□ End Date: 2012-09-05 Time: 16:11:31

__ 2. Click the **Severity** drop-down box to select the severity of alarms to capture and display (**Critical**, **Major**, or **Minor**). Or click the **All** check box to retrieve all severity levels.

__ 3. (Optional) In the **AID** box, type the AID of the entity by which you want to filter the autonomous output messages.

__ 4. (Optional) In the **Condition Type** box, type the condition type by which you want to filter the autonomous output messages.

__ 5. (Optional) Click the **Start** check box to filter the report according to a specific start time. Type the **Date** and **Time** and the respective boxes.

__ 6. (Optional) Click the **End** check box to filter the report according to a specific start time. Type the **Date** and **Time** and the respective boxes.

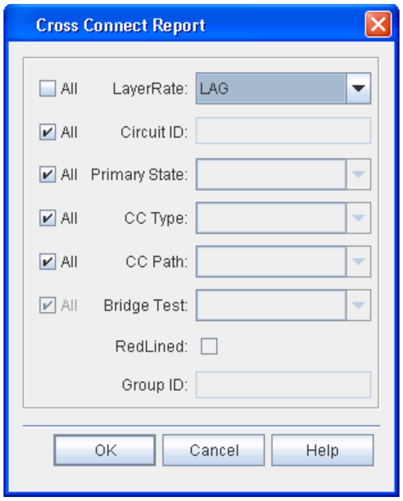
__ 7. Click **OK** to display the report.

Cross Connects Report

8.44 The Cross Connect report captures cross-connects on the NE filtered on the fields listed below. Create a Cross Connect report by performing the following steps:

__ 1. From the **Reports** menu, click **Cross Connects**. A **Cross Connect Report** dialog box displays. Refer to Figure 8.24, page 15-158.

Figure 8.24 Cross Connect Report



☐ All LayerRate: LAG

☑ All Circuit ID:

☑ All Primary State:

☑ All CC Type:

☑ All CC Path:

☑ All Bridge Test:

RedLined: ☐

Group ID:

__ 2. You can filter the Cross Connect report on the following fields:

- __ **Layer Rate**: facility/cross-connect, such as GBEP, LAG.
- __ **Circuit ID**: specific cross-connect by address.
- __ **Primary State**: cross-connects in-service or out-of-service.
- __ **CC Type**: cross-connect type.
- __ **CC Path**: path defined for cross-connect.
- __ **Bridge Test**: bridge type (such as BRIDGE or ROLL).
- __ **Group ID**: group ID if cross-connect is provisioned as OCH.

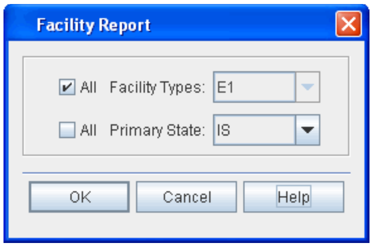
__ 3. Click **OK** to display the report.

Facilities Report

8.45 The Facility report captures facilities on the NE filtered on the fields listed below. Create a Facility report by performing the following steps:

__ 1. From the **Reports** menu, click **Facilities**. The **Facility Report** dialog box displays. Refer to Figure 8.25, page 15-158.

Figure 8.25 Facility Report



☑ All Facility Types: E1

☐ All Primary State: IS

__ 2. You can filter the facilities report on the following fields:

__ **Facility Type**: GBEP, GOPT, STMn, for example

__ **Primary State**: cross-connects in-service or out-of-service

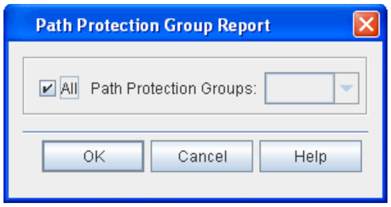
__ 3. Click **OK** to display the report.

Path Protection Group Report

8.46 The Path Protection Group (ODU SCN Protection Group) report captures PPGs on the NE filtered by the facility type. Create a Path Protection Group report by performing the following steps:

__ 1. From the **Reports** menu, click **Path Protection Group**. The **Path Protection Group Report** dialog box displays. Refer to Figure 8.26, page 15-159.

Figure 8.26 Path Protection Group Report



__ 2. Perform one of the following two options:

- Click the **All** check box to retrieve all PPGs in the NE.

or

- Click the **Path Protection Groups** drop-down box to select a facility type.

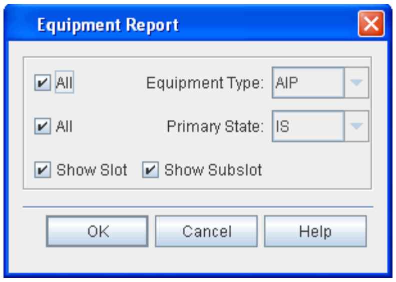
__ 3. Click **OK** to display the report.

Equipment Report

8.47 The Equipment report captures module and shelf information filtered on the fields listed below. Create an Equipment report by performing the following steps:

__ 1. From the **Reports** menu, click **Equipment**. The **Equipment Report** dialog box displays. Refer to Figure 8.27, page 15-160.

Figure 8.27 Equipment Report



Equipment Report

☑ All Equipment Type: AIP

☑ All Primary State: IS

☑ Show Slot ☑ Show Subslot

__ 2. You can filter the equipment report on the following fields:

- __ **Equipment**: Module, Pluggable Transceiver, AIP, or shelf.
- __ **Primary State**: Equipment state of in-service or out-of-service.

__ 3. Click the **Show Slot** box to display the module slot number in the equipment report.

__ 4. Click the **Show Subslot** box to display the pluggable transceiver slot number in the equipment report.

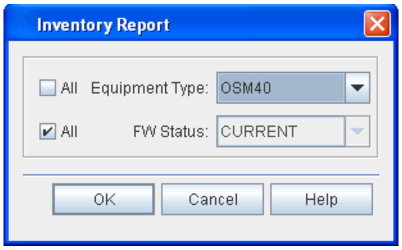
__ 5. Click **OK** to display the report.

Inventory Report

8.48 The Inventory report captures the properties of the module or modules selected. You can filter the Inventory report on modules with the most current firmware. Create an Inventory report by performing the following steps:

__ 1. From the **Reports** menu, click **Inventory**. The **Inventory Report** dialog box displays. Refer to Figure 8.28, page 15-160.

Figure 8.28 Inventory Report



Inventory Report

☐ All Equipment Type: OSM40

☑ All FW Status: CURRENT

__ 2. Click the **All** box in the **Equipment Type** field, or click the arrow button to select a specific module.

__ 3. Click the **All** box in the **Firmware Status** field, or click the arrow button to select a specific firmware state. The **Firmware Status** box displays the firmware status of the module:

- **CURRENT**: indicates that the module firmware is the latest version.
- **NOT CURRENT**: indicates that the module firmware is not the latest version.
- **NA**: indicates that the module firmware cannot be upgraded.

__ 4. Click **OK** to display the report.

__ 5. Click the **Primary State** drop-down box to select **IS** or **OSS**. Or, click the All check box to retrieve all switch domains.

__ 6. Click the **Secondary State** drop-down box to select **BUSY**, **IDLE**, **MT**, **NALMNR**, **NALMCD**, or **SGEO**. Or, click the **All** check box to retrieve all switch domains.

__ 7. Click **OK** to display the report.

Control Plane Reports

8.49 You can retrieve the following control plane reports: Call, Routing Controller Node, Topological Link, and Transitional Link.

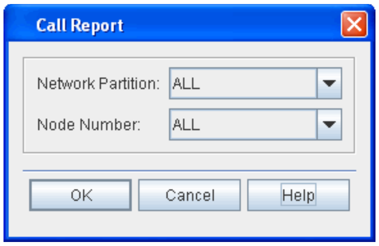
Note: *For more information about control plane, refer to Control Plane, page 15-235.*

Call Report

8.50 The Call report captures all the calls in the control plane. Create a Call report by performing the following steps:

__ 1. From the **Reports** menu, point to **Control Plane**, then click **Call**. The **Call Report** dialog box displays. Refer to Figure 8.29, page 15-161.

Figure 8.29 Call Report



Network Partition: ALL

Node Number: ALL

__ 2. Click the **Node Number** drop-down box to select the TPCP node number (**ALL**, **1–512**).

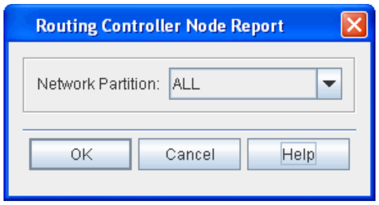
__ 3. Click **OK** to display the report.

Routing Controller Node Report

8.51 The Routing Controller Node report lists the control plane nodes that serve as routing controllers. Create a Routing Controller Node report by performing the following steps:

__ 1. From the **Reports** menu, point to **Control Plane**, then click **Routing Controller Node**. The **Routing Controller Node Report** dialog box displays. Refer to Figure 8.30, page 15-161.

Figure 8.30 Routing Controller Node Report



Network Partition: ALL

__ 2. Click the **Network Partition** drop-down box to select the network partition number (**ALL**, **2**, or **3**).

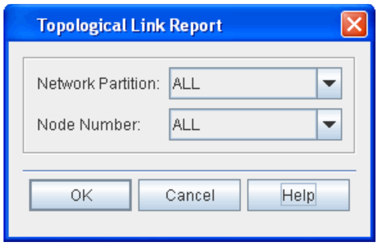
__ 3. Click **OK** to display the report.

Topological Link Report

8.52 The Topological Link report lists the topological links in the control plane. Create a Topological Link report by performing the following steps:

__ 1. From the **Reports** menu, point to **Control Plane**, then click **Topological LInk**. The **Topological Link Report** dialog box displays. Refer to Figure 8.31, page 15-162.

Figure 8.31 Topological Link Report



__ 2. Click the **Network Partition** drop-down box to select the network partition number (**ALL**, **2**, or **3**).

__ 3. Click the **Node Number** drop-down box to select the TPCP node number (**ALL**, **1–100**).

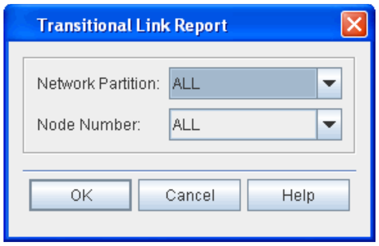
__ 4. Click **OK** to display the report.

Transitional Link Report

8.53 The Transitional Link report lists the topological links in the control plane. Create a Transitional Link report by performing the following steps:

__ 1. From the **Reports** menu, point to **Control Plane**, then click **Transitional LInk**. The **Transitional Link Report** dialog box displays. Refer to Figure 8.32, page 15-162.

Figure 8.32 Transitional Link Report



__ 2. Click the **Network Partition** drop-down box to select the network partition number (**ALL**, **2**, or **3**).

__ 3. Click the **Node Number** drop-down box to select the TPCP node number (**ALL**, **1–100**).

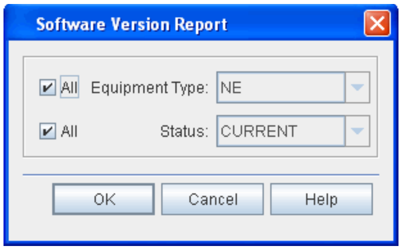
__ 4. Click **OK** to display the report.

Software Versions Report

8.54 The software versions report lists the software version for the NE. You can also retrieve the software versions for modules. Create a software versions report by performing the following steps:

__ 1. From the **Reports** menu, click **Software Versions**. The **Software Version Report** dialog box displays. Refer to Figure 8.33, page 15-163.

Figure 8.33 Software Versions Report



Software Version Report

☑ All Equipment Type: NE

☑ All Status: CURRENT

__ 2. Click the **All** box in the **Equipment Type** field, or click the arrow button to select a specific module.

__ 3. Click the **All** box in the **Status** field, or click the arrow button to select a specific state.

- **CURRENT**: indicates that the module firmware is the latest version.
- **NOT CURRENT**: indicates that the module firmware is not the latest version.

__ 4. Click **OK** to display the report.

Managing the Reports

8.55 The menus in the **Print Preview** window provide actions for managing the data in the report and the report display. The **File** menu allows you to export, save, or print data in the report. The **Navigation** menu provides tools for moving through multi-page reports. The **Zoom** menu provides screen control so you can increase or decrease element size.

Capturing the Data

8.56 You can print, save, or export the information provided in the reports.

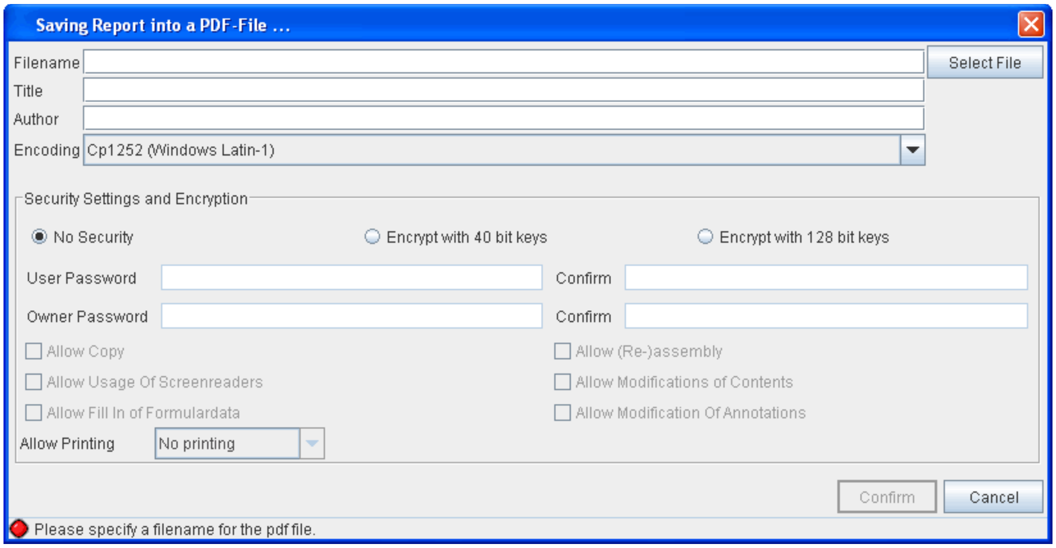
Saving the Data

8.57 Save the report as a PDF file by performing the following steps:

__ 1. At the top of the **Print Preview** window, click the **File** menu.

__ 2. Click **Save as PDF**. The **Saving Report into a PDF-File** dialog box displays. Refer to Figure 8.34, page 15-164.

Figure 8.34 Saving Report into a PDF



Saving Report into a PDF-File ...

Encoding: Cp1252 (Windows Latin-1)

Security Settings and Encryption: ● No Security ○ Encrypt with 40 bit keys ○ Encrypt with 128 bit keys

Allow Printing: No printing

Please specify a filename for the pdf file.

Filename
Select File
Title
Author
User Password
Confirm
Owner Password
Confirm
□ Allow Copy
□ Allow (Re-)assembly
□ Allow Usage Of Screenreaders
□ Allow Modifications of Contents
□ Allow Fill In of Formulardata
□ Allow Modification Of Annotations
Confirm
Cancel

__ 3. Type a **Filename**.

__ 4. (optional) Type the **Title** of the report.

__ 5. Verify the information in the **Author** box. (The **Author** box defaults to the current user's login.)

__ 6. Accept the default setting for **Encoding** (Cp1252 (Windows Latin-1)).

__ 7. (optional) In the **Security Settings and Encryption** box, you can set access and printing security on the report. Click **No Security** to allow all users printing and modification privileges. Click **Encrypt with 40 bit keys** or **Encrypt with 128 bit keys** to restrict printing and modification actions by users other than the author. If you select one of the encryption settings, complete the following fields:

__ 7.1 Type and Confirm the **User Password** of the user to whom you grant access.

__ 7.2 Type and Confirm the **Owner Password** of the user who created the report.

__ 7.3 To enable report setting select the following options. The user identified in User Password can use any selection enabled.

- Allow Copy
- Allow Usage of Screenreaders
- Allow Fill In of Formular data

- Allow Re-assembly
- Allow Modification of Contents
- Allow Modification of Annotations
- Allow Printing

__ 8. Click **Confirm** to apply all settings.

Note: *To allow printing with No Security, click one of the encryption selections, then select a printing option at the Allow Printing box. After setting the print option, deselect the encryption button, and click No Security.*

__ 9. Type a **Filename**, or click **Select File**, and browse to an existing file to overwrite.

__ 10. Click the applicable print driver that converts the report into a text file: **Plain text output**, **Epson ESC/P compatible**, **IBM compatible**. (The typical selection is **Plain text output**.)

__ 11. Accept the default setting for **Encoding** (Cp1252 (Windows Latin-1)).

__ 12. Accept or modify the **Font settings** using the drop-down boxes.

__ 13. Click **Confirm** to apply all settings.

Exporting the Data

8.58 The Craft Station supports four formats for exporting data: Excel, rich text format (RTF), hypertext markup language (HTML), and comma separated value (CSV).

8.59 The fields that display are standard for each format type and should be completed according to your corporate standards. If you are not sure of a setting, accept the default.

Viewing Alarms and Events in Alarm Window

8.60 The **Alarm Window** displays all of the current alarms and the following alarm information: severity, the associated NE, object in alarm, detailed location of object (AID), type of alarm, if the alarm is service affecting, the time and date the alarm was set, sequence in current alarms set, a description of the alarm condition, and any user-defined location identifiers. New alarms display as they are set. When the problem condition that set the alarm clears, the alarm no longer displays in the **Alarm Window**.

8.61 The **Event Window** displays all of the current events and the following event information: sequence, the associated NE, object in event, detailed location of object, a description of the event, the current state of the object, the time and date the event was set, and any user-defined location identifiers. New events display as they are set.

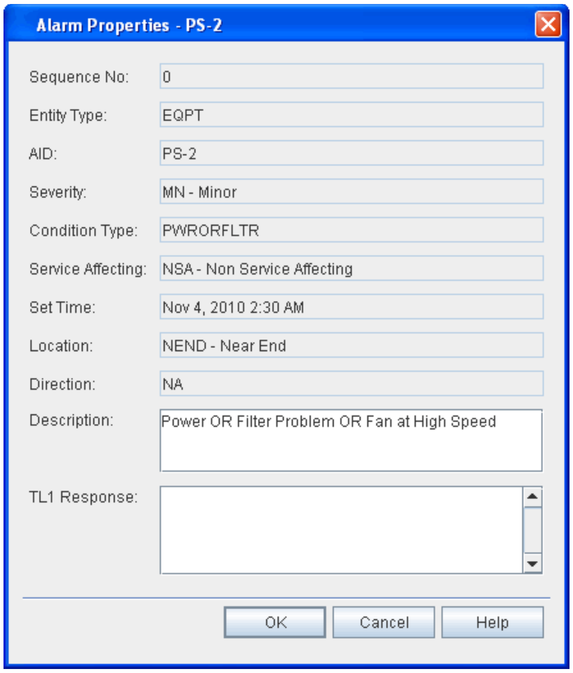
Viewing Alarm Properties

8.62 View the details of any alarm in the **Alarm Window** by double-clicking the item. View alarm details by performing the following steps:

__ 1. Select one alarm in the **Alarm Window**.

__ 2. Double-click the selected alarm. An **Alarm Properties** dialog box displays. Refer to Figure 8.35, page 15-166.

Figure 8.35 Alarm Properties



Alarm Properties - PS-2

Sequence No: 0

Entity Type: EQPT

AID: PS-2

Severity: MN - Minor

Condition Type: PWRORFLTR

Service Affecting: NSA - Non Service Affecting

Set Time: Nov 4, 2010 2:30 AM

Location: NEND - Near End

Direction: NA

Description: Power OR Filter Problem OR Fan at High Speed

TL1 Response:

The following fields display:

- **Sequence No.**: sequence in alarm list
- **Entity Type**: shelf, module, facility, router
- **AID**: the system address of the entity
- **Severity**: severity of alarm: critical, major, minor
- **Condition Type**: identifies nature of alarm
- **Service Affecting**: indicates if alarm is service affecting (SA) or not (NSA)
- **Set Time**: time of day, month, and year when alarm was set
- **Location**: alarm was set at near-end or far-end of network
- **Direction**: identifies transmit direction of signal:
  - **TDTC**: transmit direction toward customer
  - **TDTN**: transmit direction toward DWDM network
  - **NA**: not applicable

- **Description**: brief description of the alarm type
- **TL1 Response**: alarm response expressed in TL1

Viewing Events

8.63 View the details of any event in the **Event Window** by double-clicking the item. View event details by performing the following steps:

__ 1. Select one event in the **Event Window**.

__ 2. Double-click the selected event. An **Event Properties** dialog box displays.

The following fields display:

- **Sequence No.**: sequence in event list
- **Entity Type**: shelf, module, facility, router
- **AID**: the system address of the affected entity
- **Condition Eff**: the effect of the event on the condition:
  - **TC** = transient condition
  - **SC** = standing condition
  - **CL** = cleared condition
- **Condition Type**: identifies nature of event (for instance, **DBCHG** indicates a database change)
- **Command Type**: equivalent TL1 command
- **State**: present state of the entity
- **Set Time**: time of day, month and year when event was set
- **Location**: alarm was set at near-end or far-end of network
- **Direction**: identifies transmit direction of signal:
  - **TDTC**: transmit direction toward customer
  - **TDTN**: transmit direction toward DWDM network
  - **NA**: not applicable
- **Description**: brief description of the alarm type
- **TL1 Response**: event response expressed in TL1

Alarm Reporting Control

8.64 When you enable the alarm reporting control (ARC) feature, alarm reporting turns off for the specified transponder or facility to allow provisioning, testing, or maintenance of the transponder circuit without generating a flood of alarms. Define a period of time for alarm reporting control (ARC) to be in effect. When the period expires, the alarm state of the transponder or facility returns to normal operating state (reporting alarms).

8.65 When ARC is enabled, standing alarms, events, and threshold crossing alerts (TCAs) are not reported in the software or displayed visually on the alarm interface panel (AIP). Alarms set before ARC was enabled are reported if the state changes to cleared. Some transient events, such as protection switch events, are also reported.

8.66 The ARC feature supports the following transponders: OSM-2C, OSM-1S, and OSM-2S. When provisioned on these modules, ARC disables both line-side and port-side facility alarms.

8.67 The following facilities support the ARC feature: HGE, OCH-P, ODUF, OTU1, OTU4, STM64, and TGLAN.

8.68 Alarm reporting control supports two states: Qualified Inhibition (**QI**) and Release (**RLS**). Qualified Inhibition indicates if alarms are suppressed and is set for a specific period of time in minutes and/or hours. You can set hours (**hh**) in the range of 0 to 99, and minutes (**mm**) in the range of 0 to 59. The default value is 8:00 (eight hours).

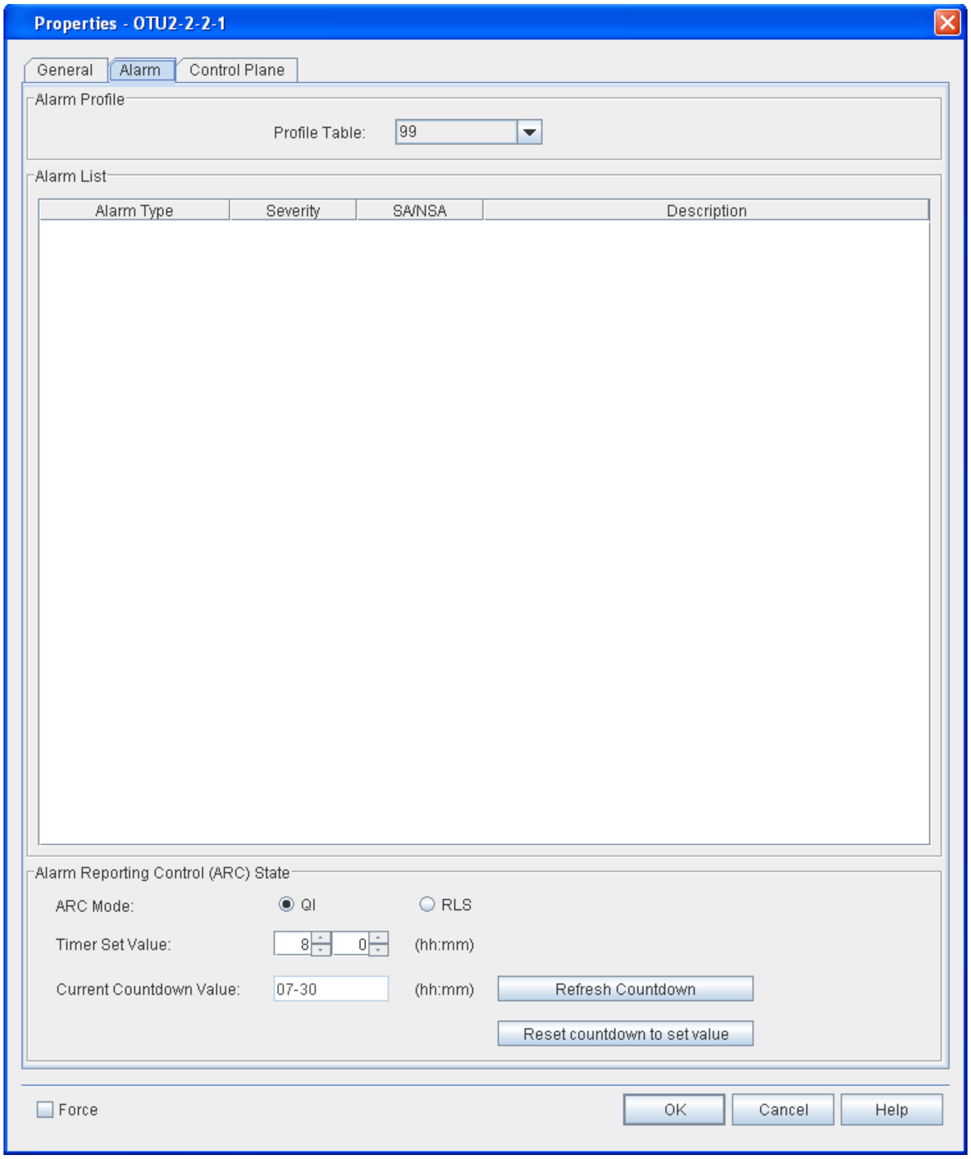
8.69 The system software interface (element manager, Craft Station, or TL1) reports both the original duration of the inhibited period and the time remaining in the period. The inhibition period starts only when an error-free signal is detected and the entity is in Not Alarmed Count Down (NALMCD). If a defect is detected during the inhibition period, the counter stops and waits until the signal is error-free again. When an error-free signal is again detected, the counter resets and restarts the inhibition period from the provisioned interval value.

8.70 Provision the ARC feature by performing the following steps:

__ 1. In the **Navigation Window**, right-click the transponder or facility to view the shortcut menu, then click **Properties**. The **Properties** dialog box displays.

__ 2. Click the **Alarm** tab. The **Alarm Report Control** feature displays on the **Alarm** tab. Refer to Figure 8.36, page 15-169.

Figure 8.36 Alarm Reporting Control



Profile Table: 99

Alarm Type	Severity	SA/NSA	Description

ARC Mode: ● QI ○ RLS

Timer Set Value: 8 0 (hh:mm)

Current Countdown Value: 07-30 (hh:mm)

□ Force

__ 3. To start **ARC Mode**, click the **QI** button.

__ 4. Click in the **Timer Set Value** box, and select the time period that ARC will be enabled using the arrows. The hour value range allowed is **0–99**; the minute value range allowed is **0–59**. The system default interval is **8-00**.

__ 5. Click **OK** to start the ARC interval.

__ 6. To review how much time remains in an ARC interval, view the **Current Countdown Value** button.

__ 7. To turn off the ARC feature, click the **RLS** button. The Craft Station reports alarms on the entity.

__ 8. Click **OK**.

Alarm Generation

8.71 Use the alarm generation feature to generate all possible alarms for all entities provisioned in a system. The NE generates alarms for a provisioned entity regardless of the state of the entity (such as OOS or ARC). You can select or deselect entities to alarm based on whether they are provisioned or not.

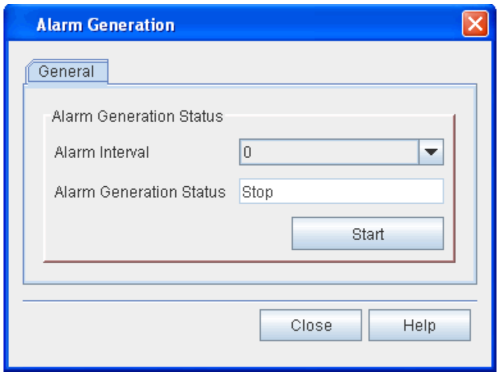
8.72 When you use the alarm generation feature, the NE issues a REPT^ALM for each alarm generated and cleared. But, when an alarm is generated against the entity, its state and associated LED do not change. Therefore, the NE does not issue a REPT^DBCHG because the entities do not change state.

8.73 When you stop the alarm generation feature, the NE re-posts actual system alarms with the timestamp of their occurrence.

Note: *You can use the alarm generation feature to perform alarm testing on an operational system in order to verify Craft Station operation.*

__ 1. In the **Navigation Window**, right-click the NE icon to view the shortcut menu, then click **Alarm Generation**. The **Alarm Generation** dialog box displays. Refer to Figure 8.37, page 15-170.

Figure 8.37 Alarm Generation



Alarm Interval: 0

Alarm Generation Status: Stop

__ 2. Click the **Alarm Interval** drop-down box to select the interval at which the NE displays alarms (**0**, **1**, **2**, **4**, **8**, **16**, **32**, or **64** seconds).

__ 3. Click **Start** to start alarm generation. A **Confirmation** box displays to indicate that the NE started the alarm generation. Click **OK.** The **Alarm Generation Status** box displays "Generating Alarms."

__ 4. Alarms scroll in the alarm window.

__ 5. Click **Stop** to stop alarm generation. An **Information** box displays to indicate that the alarm generation process has stopped. Click **OK**.

Network Diagnostics

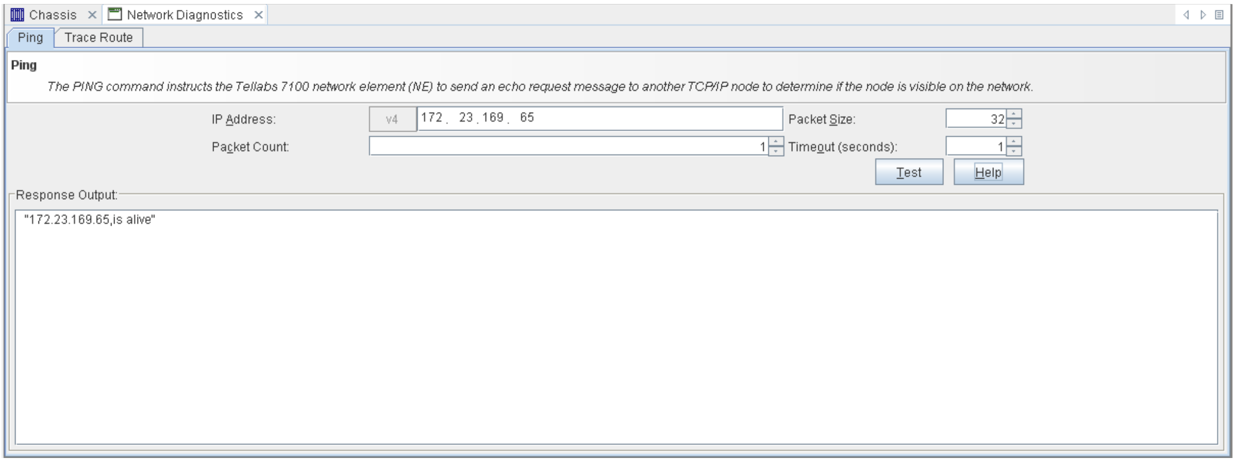
8.74 The Craft Station offers two network diagnostic features: ping and trace route. The ping feature instructs the NE to send an echo request message to another TCP/IP node to determine if the node is visible on the network. The trace route feature instructs the NE to send probe packets that attempt to trace a path to the destination node.

Ping

8.75 Determine if a node is visible on the network by performing the following steps:

__ 1. In the **Navigation Window**, right-click the NE to view the shortcut menu, point to **Network Diagnostics**, then click **Ping**. The **Network Diagnostics** window displays. Refer to Figure 8.38, page 15-171.

Figure 8.38 Ping



Ping

The PING command instructs the Tellabs 7100 network element (NE) to send an echo request message to another TCP/IP node to determine if the node is visible on the network.

IP Address: v4 172 . 23 . 169 . 65

Packet Size: 32

Packet Count: 1

Timeout (seconds): 1

Response Output:

```
"172.23.169.65,is alive"
```

__ 2. Verify the **Ping** tab is selected.

__ 3. In the **IP Address** box, type the IP address of another TCP/IP node on the network using the IPv4 or IPv6 address format.

- IPv4 address = "www.xxx.yyy.zzz"

Where:

w, **x**, **y**, **z** = **0–9**

www, **xxx**, **yyy**, **zzz** = **0-255**

The following IPv4 addresses are not allowed:
"224-255.xxx.xxx.xxx"
"169.254.xxx.xxx"
"127.xxx.xxx.xxx"
"10.0.0–3.xxx"
"0–1.xxx.xxx.xxx"

- IPv6 address = "x:x:x:x:x:x:x:x"

Where:

x = **0000**-**FFFF** (1–4 hexadecimal digits). The zero compression format is also supported (a double colon "::" indicates one or more groups of 16 bits of zeros).
The following IPv6 addresses are not allowed: "0:0:0:0:0:0:0:1"

__ 4. Click the **Packet Count** up- and down- arrows to set the packet count (**1**–**32**).

__ 5. Click the **Packet Size** up- and down-arrows to set the packet size (**0**–**1024**).

__ 6. Click the **Timeout (seconds)** up- and down- arrows to set the time before giving up on an echo response from the NE (**1**–**5**).

__ 7. Click **Test**.

__ 8. View the results of the network diagnostic test in the **Response Output** area.

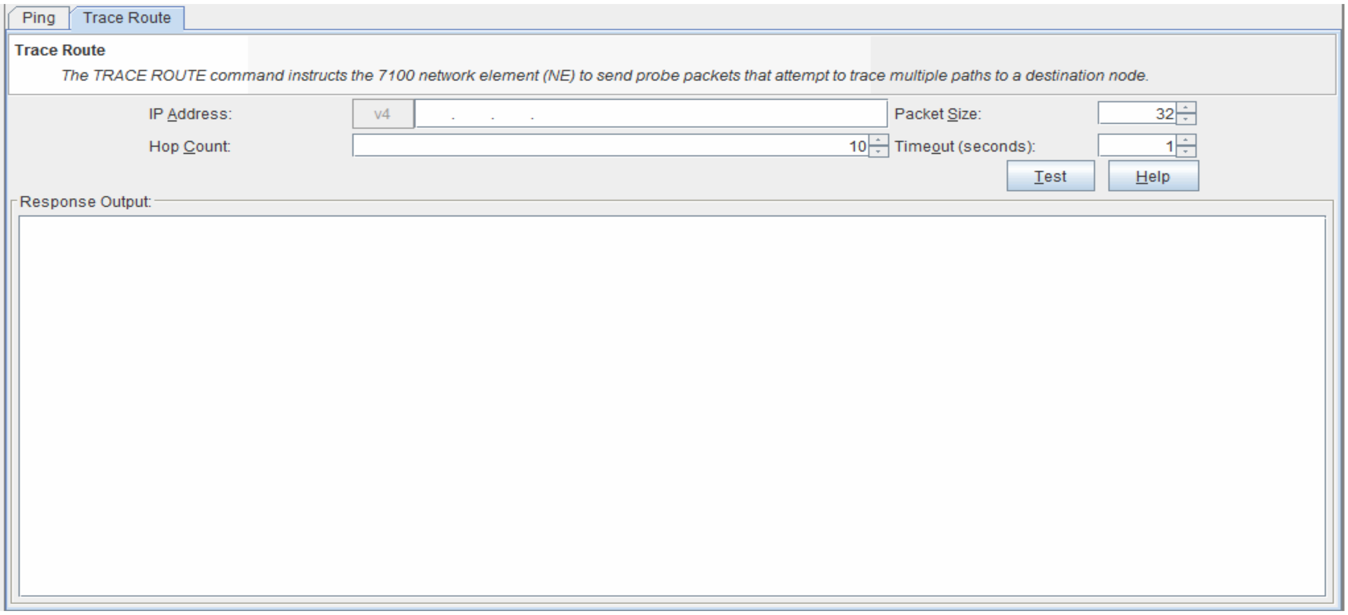
Trace Route

8.76 Initiate a trace route by performing the following steps:

__ 1. In the **Navigation Window**, right-click the NE to view the shortcut menu, point to **Network Diagnostics**, then click **Ping**. The **Network Diagnostics** window displays.

__ 2. Click the **Trace Route** tab. refer to Figure 8.39, page 15-172.

Figure 8.39 Trace Route



Trace Route

The TRACE ROUTE command instructs the 7100 network element (NE) to send probe packets that attempt to trace multiple paths to a destination node.

IP Address: v4 . . .

Packet Size: 32

Hop Count: 10

Timeout (seconds): 1

__ 3. In the **IP Address** box, type the IP address of the destination node using the IPv4 or IPv6 address format.

- IPv4 address = "www.xxx.yyy.zzz"

Where:

w, **x**, **y**, **z** = **0**–**9**

www, **xxx**, **yyy**, **zzz** = **0**-**255**

The following IPv4 addresses are not allowed:
"224-255.xxx.xxx.xxx"
"169.254.xxx.xxx"
"127.xxx.xxx.xxx"
"10.0.0–3.xxx"
"0–1.xxx.xxx.xxx"

- IPv6 address = "x:x:x:x:x:x:x:x"

Where:

x = **0000**-**FFFF** (1–4 hexadecimal digits). The zero compression format is also supported (a double colon "::" indicates one or more groups of 16 bits of zeros).

The following IPv6 addresses are not allowed:
"0:0:0:0:0:0:0:1"

__ 4. Click the **Hop Count** up- and down- arrows to specify the number of hops that the trace route message will traverse (**1**–**32**).

__ 5. Click the **Packet Size** up- and down-arrows to set the packet size (**0**–**1024**).

__ 6. Click the **Timeout (seconds)** up- and down- arrows to set the time before giving up on an echo response from the NE (**1**–**5**).

__ 7. Click **Test**.

__ 8. View the results of the network diagnostic test in the **Response Output** area.

9. Provisioning Modules

9.1 This section describes creating and provisioning modules. Refer to *System Engineering* for detailed descriptions of the modules and how they are located within the NE.

Modules Supported in FP1.0

9.2 Refer to *FP1.0.x Software Release Document* for modules supported in FP1.0.x.

9.3 Create modules in the Craft Station software by right-clicking the shelf in the Navigation Window, or by right-clicking an empty slot in the Chassis View.

9.4 Autodiscovery identifies modules at system turn-up. Autodiscovered modules require no intervention to be provisioned. The NE does not autodiscover filler modules when they are inserted into a shelf.

Note: *Refer to ENT-EQPT::x command in TL1 Command Reference Manual for additional details on modules. Click the Help menu in the Craft Station to access this document.*

Provisioning Modules

9.5 This section describes provisioning activities for modules. The system auto-discovers most modules. You can also create modules by right-clicking the main shelf or port shelf icon or by right-clicking a shelf slot in the **Chassis View** and selecting **Create Module**. In the **Create Module** dialog box, only empty slots display in the **Slot** field. When a slot is selected, only the modules eligible for that slot display in the **Module Type** field.

9.6 The following fields in the **Create Module** dialog box are common to all modules: type, slot number, name, alarm profile, and management state. Other fields apply to specific modules.

9.7 This section describes the **Create Module** dialog box. You can right-click any shelf, and select **Create Module** from the shortcut menu to preprovision a module.

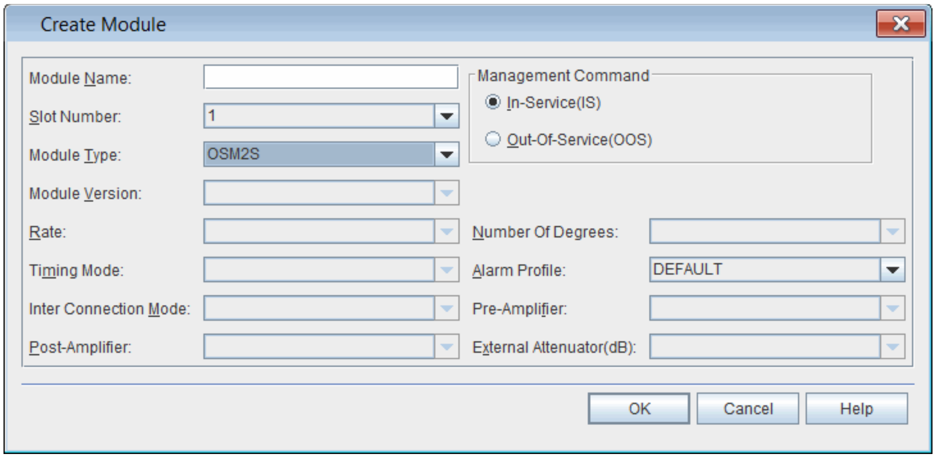
Note: *Refer to TL1 Command Reference Manual for more information about provisioning other types of modules. Click the Help menu in the Craft Station to access this document.*

Optical Transport Network Switching Module - 2S (OSM-2S)

9.8 Provision a switching module, for example an OSM-2S, by performing the following steps:

__ 1. In the **Navigation Window**, right-click the port shelf to view the shortcut menu, then click **Create Module**. The **Create Module** dialog box displays. Refer to Figure 9.1, page 15-175.

Figure 9.1 Create Module (OSM2S)



Create Module

Module Name:

Slot Number: 1

Module Type: OSM2S

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

Module Version:

Rate:

Number Of Degrees:

Timing Mode:

Alarm Profile: DEFAULT

Inter Connection Mode:

Pre-Amplifier:

Post-Amplifier:

External Attenuator(dB):

__ 2. Click the **Slot Number** drop-down box to select a slot number.

__ 3. Click the **Module Type** drop-down box to select **OSM2S**.

__ 4. (optional) Type a name for the OSM-2S in the **Module Name** box.

__ 5. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 6. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0–20**, **99**).

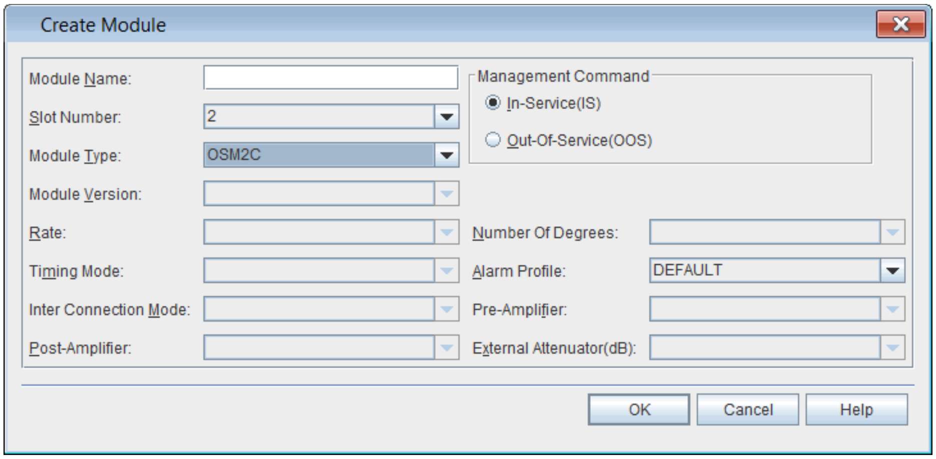
__ 7. Click **OK**. An icon labeled **OSM2S** displays below the shelf icon in the **Navigation Window**.

Optical Transport Network Switching Module - 2C (OSM-2C)

9.9 Provision a switching module, for example an OSM-2C, by performing the following steps:

__ 1. In the **Navigation Window**, right-click the port shelf to view the shortcut menu, then click **Create Module**. The **Create Module** dialog box displays. Refer to Figure 9.2, page 15-176.

Figure 9.2 Create Module (OSM2C)



Create Module

Module Name:

Slot Number: 2

Module Type: OSM2C

Module Version:

Rate:

Timing Mode:

Inter Connection Mode:

Post-Amplifier:

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

Number Of Degrees:

Alarm Profile: DEFAULT

Pre-Amplifier:

External Attenuator(dB):

__ 2. Click the **Slot Number** drop-down box to select a slot number.

__ 3. Click the **Module Type** drop-down box to select **OSM2C**.

__ 4. (optional) Type a name for the OSM-2C in the **Module Name** box.

__ 5. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 6. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0**–**20**, **99**).

__ 7. Click **OK**. An icon labeled **OSM2C** displays below the shelf icon in the **Navigation Window**.

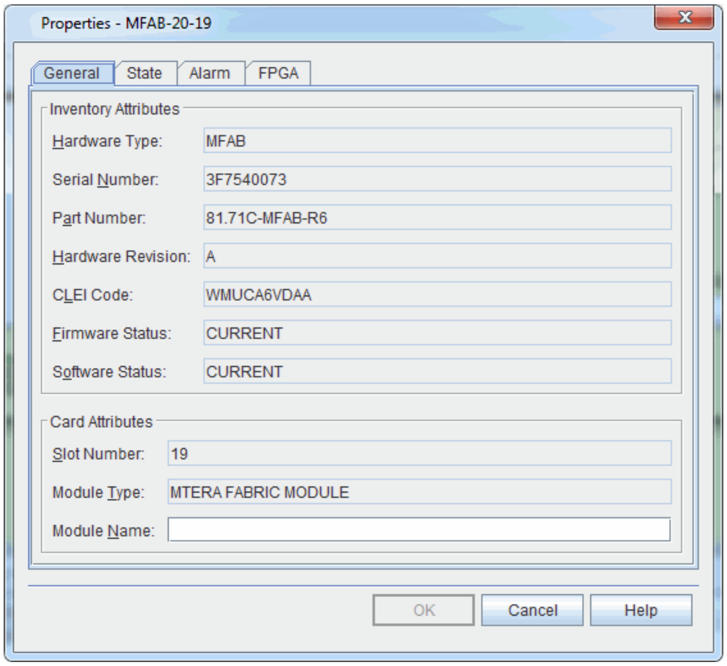
mTera Fabric Module (MFAB)

9.10 The mTera automatically pre-provisions six MFABs per shelf. View the properties of the MFAB by performing the following steps:

__ 1. In the **Navigation Window**, right-click the MFAB to view the shortcut menu, then click **Properties**. The **Properties** dialog box displays.

__ 2. Verify that the **General** tab is selected. Refer to Figure 9.3, page 15-177.

Figure 9.3 Properties - MFAB



Inventory Attributes

Hardware Type: MFAB

Serial Number: 3F7540073

Part Number: 81.71C-MFAB-R6

Hardware Revision: A

CLEI Code: WMUCA6VDAA

Firmware Status: CURRENT

Software Status: CURRENT

Card Attributes

Slot Number: 19

Module Type: MTERA FABRIC MODULE

Module Name:

__ 3. Verify the following attributes:

- **Hardware Type**
- **Serial Number**
- **Part Number**
- **Hardware Revision**
- **CLEI Code**
- **Firmware Status**
- **Software Status**
- **Slot Number**
- **Module Type**

__ 4. (optional) Type a name for the MFAB in the **Module Name** box.

State Tab

__ 5. Click the **State** tab.

- In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.
- In the **Command Mode** area, click **Forced** or **Normal**.

Note: *Click* ***Forced*** *if you want to ignore impact on traffic and suppress alarms, events and other system messages that describe the consequences of the action. Click* ***Normal*** *if you want to view alarms, events, and other system messages that describe the consequences of the action.*

__ 6. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0–20**, **99**).

__ 7. View any alarms in the **Alarm List**.

FPGA Tab

__ 8. Click the **FPGA** tab.

__ 9. View the FPGA information.

__ 10. Click **OK**.

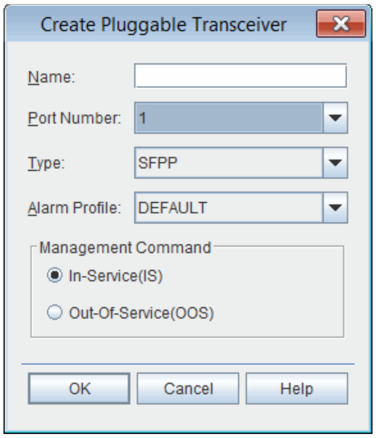
Creating Pluggable Transceiver

9.11 The Craft Station automatically creates an icon for a pluggable transceiver when you insert the device into a module. You can provision new pluggable transceivers on multi-port transponder modules or switching modules after a pluggable device has been deleted. (The available ports and ability to provision either SFPPs or CFPs depends on the type of multi-port transponder.) You can also pre-provision a pluggable transceiver. (If you pre-provision a pluggable transceiver, the properties of the device display after you insert the device into the module.)

9.12 Provision a pluggable transceiver on a multi-port module by performing the following steps:

__ 1. In the **Navigation Window**, right-click the module to view the shortcut menu, then click **Create Pluggable Transceiver**. The **Create Pluggable Transceiver** dialog box displays. Refer to Figure 9.4, page 15-178.

Figure 9.4 Create Pluggable Transceiver



Create Pluggable Transceiver

Name:

Port Number: 1

Type: SFPP

Alarm Profile: DEFAULT

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

__ 2. (optional) Type a name for the pluggable transceiver in the **Name** box.

__ 3. Click the **Port Number** drop-down box to select the port number.

__ 4. Click the **Type** drop-down box to select **SFPP or CFP**.

__ 5. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0**–**20**, **99**).

__ 6. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 7. Click **OK**. A labeled icon displays in the **Navigation Window** underneath the module.

Managing SFPP Components

9.13 When equipped in a module, view the form-factor pluggables available for multi-port modules in the **Navigation Window**.

9.14 View the properties of a pluggable transceiver by performing the following steps:

__ 1. Click the related module to expand it. The provisioned **SFPP** entities display.

__ 2. Right-click the **SFPP** to view the shortcut menu, then click **Properties**. The **Properties** dialog displays.

__ 3. Click the **General** tab to view the following parameters:

- **Name**: user-defined name
- **Port Number**: module port where pluggable transceiver is located
- **Type**: pluggable type (**SFPP**)
- **Channel Number**: NA
- **Wavelength (nm)**: NA
- **HW Revision**: revision letter of pluggable transceiver
- **Serial Number**: serial number assigned to pluggable transceiver
- **CLEI Code**: CLEI code assigned to pluggable transceiver
- **Part Number**: pluggable transceiver part number

__ 4. Click the **State** tab to manage the state of the pluggable transceiver:

- In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.
- In the **Command Mode** area, click **Forced** or **Normal**.

Note: *Click **Forced** if you want to ignore impact on traffic and suppress alarms, events and other system messages that describe the consequences of the action. Click **Normal** if you want to view alarms, events, and other system messages that describe the consequences of the action.*

__ 5. Click the **Alarm** tab to view alarms posted against the pluggable transceiver.

Managing CFP Components

9.15 When equipped in a module, view the form-factor pluggables available for multi-port modules in the **Navigation Window**.

9.16 View the properties of a pluggable transceiver by performing the following steps:

__ 1. Click the related module to expand it. The provisioned **CFP** entity displays.

__ 2. Right-click the **CFP** to view the shortcut menu, then click **Properties**. The **Properties** dialog displays.

__ 3. Click the **General** tab to view the following parameters:

- **Name**: user-defined name
- **Port Number**: module port where pluggable transceiver is located (1 or 2)
- **Type**: pluggable type (**CFP**)
- **HW Revision**: revision letter of pluggable transceiver
- **Serial Number**: serial number assigned to pluggable transceiver
- **CLEI Code**: CLEI code assigned to pluggable transceiver
- **Part Number**: pluggable transceiver part number

__ 4. Click the **State** tab to manage the state of the pluggable transceiver:

- In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.
- In the **Command Mode** area, click **Forced** or **Normal**.

Note: *Click **Forced** if you want to ignore impact on traffic and suppress alarms, events and other system messages that describe the consequences of the action. Click **Normal** if you want to view alarms, events, and other system messages that describe the consequences of the action.*

__ 5. Click the **Alarm** tab to view alarms posted against the pluggable transceiver.

Deleting Pluggable Transceiver

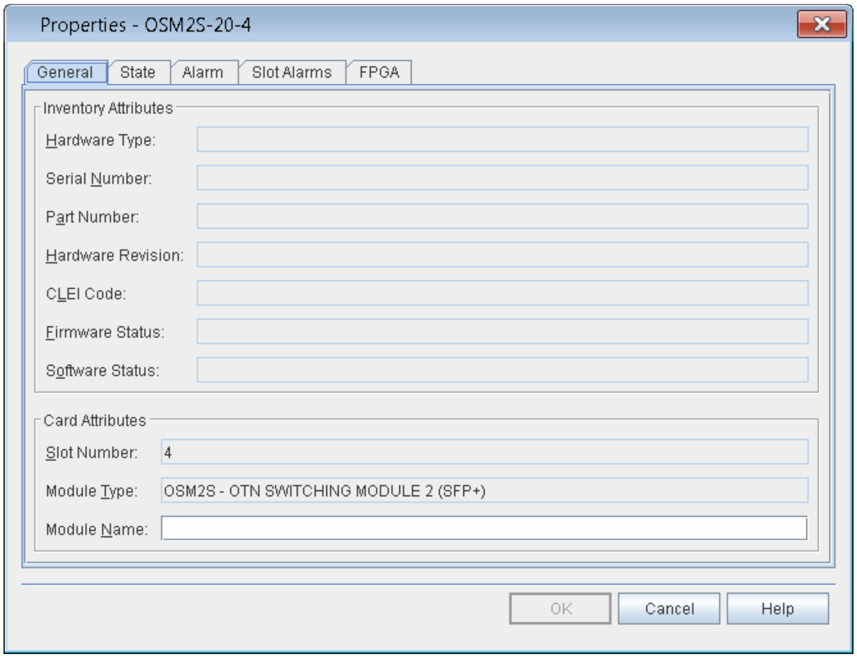
Note: *Before you delete a pluggable transceiver, delete the facility supported by the pluggable transceiver.*

9.17 Right-click the pluggable transceiver to view the shortcut menu, then click **Delete** to delete the CFP or SFPP.

Module and Fan Properties

9.18 In the Craft Station, you can right-click a module or fan and review its properties via a shortcut menu. Choose **Properties** from the shortcut menu to review current settings. Refer to the examples shown in Figures 9.5, page 15-181 through 9.6, page 15-181.

Figure 9.5 Example Module Properties (OSM2S)



Properties - OSM2S-20-4

Inventory Attributes

Hardware Type:

Serial Number:

Part Number:

Hardware Revision:

CLEI Code:

Firmware Status:

Software Status:

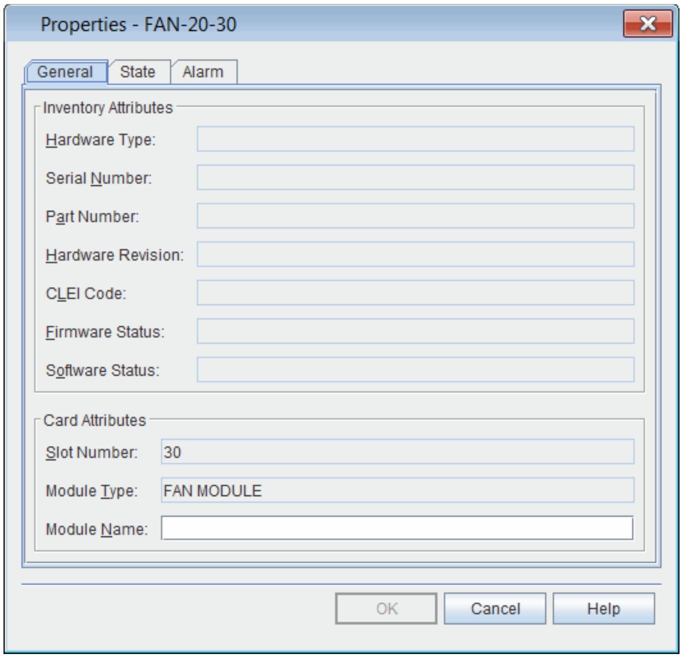
Card Attributes

Slot Number: 4

Module Type: OSM2S - OTN SWITCHING MODULE 2 (SFP+)

Module Name:

Figure 9.6 Example of mTera Properties - FAN



Properties - FAN-20-30

Inventory Attributes

Hardware Type:

Serial Number:

Part Number:

Hardware Revision:

CLEI Code:

Firmware Status:

Software Status:

Card Attributes

Slot Number: 30

Module Type: FAN MODULE

Module Name:

9.19 The following information displays in the module properties dialog box. You can provision the present state of the module and the module description. To access module properties, right-click any module to view the shortcut menu, then click **Properties**.

- **Hardware Type**: module acronym
- **Serial Number**: the serial number assigned to the module
- **Part Number**: the part number of the module
- **Hardware Revision**: the revision of the module; typically A or B
- **CLEI Code**: Common Language Equipment Identification
- **Firmware Status**: indicates if the firmware on the module is the latest available
  - **CURRENT**: indicates that the module firmware is the latest version
  - **NOT CURRENT**: indicates that the module firmware is not the latest version
  - **NA**: indicates that the module firmware cannot be upgraded
- **Software Status**: indicates if the firmware on the module is the latest available
  - **CURRENT**: indicates that the module software is the latest version
  - **NOT CURRENT**: indicates that the module software is not the latest version
  - **NA**: indicates that the module software cannot be upgraded
- **Slot Number**: slot number of the module
- **Module Type**: full name of module, such as System Processor Module
- **Module Name**: user-defined name of module
- **Channel Number**: Indicates the channel number corresponding to the wavelength supported by a fixed DWDM XFP. If the XFP is not a fixed DWDM XFP, the value returned will be NA.

9.20 Click the **State** tab to display the state of the module.

- **Primary State**: Current state of module: in service (IS) or out of service (OOS). A further qualifier may display as described below:
  - **NR**: normal
  - **ANR**: abnormal
  - **RST**: restricted
  - **ANRST**: abnormal and restricted
  - **AU**: autonomous
  - **MA**: management
  - **AUMA**: autonomous and management

  - **AURST**: autonomous and restricted
  - **MAANR**: management and abnormal
- **Secondary State** of module:
  - **ACTIVE**: active
  - **APR**: automatic power reduction
  - **DGN**: diagnostic
  - **FLT**: fault
  - **MEA**: mismatch of equipment and attributes
  - **MT**: maintenance
  - **NALMQI**: not alarmed qualified inhibit
  - **PMI**: performance monitoring inhibited
  - **PWR**: power
  - **STBY**: standby
  - **SWDL**: software download
  - **TMGMASTER**: Master Timing Source
  - **TMGSLAVE**: Slave Timing Source
  - **UEQ**: unequipped
- **Management Command**
  - In-Service(IS)
  - Out-Of-Service(OOS)
- **Command Mode**
  - Normal
  - Forced

9.21 Click the **Alarm** tab to view any alarms that may exist on the module.

Note: *If the module supports the Alarm Reporting Control (ARC) feature, refer to Alarm Reporting Control, page 15-168 for information about alarm profile and ARC parameters.*

9.22 Click the **Slot Alarms** tab to view any alarms that may exist on an pluggable transceiver of a multi-port module.

9.23 Click the **FPGA** tab to view the following information about the FPGA supported on the module: name, version, and status.

Managing the Module State

9.24 You can modify the module state. Right-click the module in the **Navigation Window** to view the shortcut menu, point to **Module**, then click one of the following options:

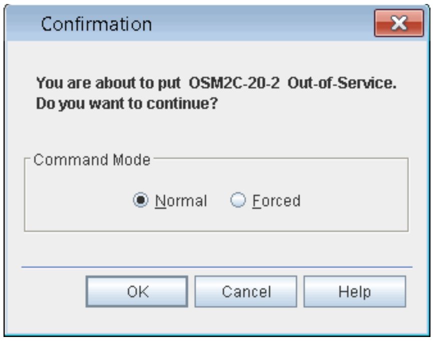
- **Reset**: Forces a reset of the module. A **Warm Start** consists of a software reset; a **Cold Start** consists of a hardware reset. The System Processor Module (SPM) supports the **Shutdown** parameter. The Shutdown option powers down the SPM or SPM-N until you initiate a cold start.
- **Edit Out-Of-Service (OOS-MA)**: Sets the state of the module to out-of-service (maintenance).

Note: *When you place a module out-of-service, the system automatically places all of the facilities supported on that module out-of-service.*

- **Edit In-Service (IS from OOS-MA)**: Changes the state of the module from out-of-service maintenance to in-service.

9.25 After each action, a **Confirmation** box displays. Refer to Figure 9.7, page 15-184. For modules that support the normal and forced command mode, the **Confirmation** box that displays for **Edit Out-Of-Service** includes a selection for **Normal** or **Forced**. Select **Forced** if you want to ignore impact on traffic and suppress alarms, events, and other system messages that describe the consequences of the action. Select **Normal** if you want to view alarms, events, and other system messages that describe the consequences of the action.

Figure 9.7 Confirmation to Change Module State Using Normal Command Mode



Confirmation

You are about to put OSM2C-20-2 Out-of-Service.
Do you want to continue?

Command Mode

● Normal ○ Forced

Deleting Modules

9.26 Delete a module by performing the following steps:

Note: *Before you delete a module, delete all facilities and direct connections associated with the module. Then set the module state to OOS.*

__ 1. Right-click the selected module icon in the **Navigation Window** to view the shortcut menu, then click **Delete**.

__ 2. A **Confirmation** box displays. Click **OK** or **Cancel**.

External Connections (Direct Connect)

9.27 The Direct Connect feature provides a direct path between the line-side optical channel on an mTera module and a DWDM multiplexer that is external to the mTera. The channel mimics a foreign wavelength, allowing a single wavelength connection to external equipment without provisioning the path through a DWDM multiplexer (CMM-44, CCM-xR, OADM-xR, or RCMM-xR). The line-side G.709 signal on the module is tuned to one of the channels supported on the 7100 OTS/7100 Nano. The OSM-2S and OSM-2C support the Direct Connect feature. Refer to the individual module practice for information about the line-side optical transmit power level and the receiver sensitivity on the modules that support the Direct Connect feature.

9.28 For more information about planning an external connection, refer to *System Engineering*.

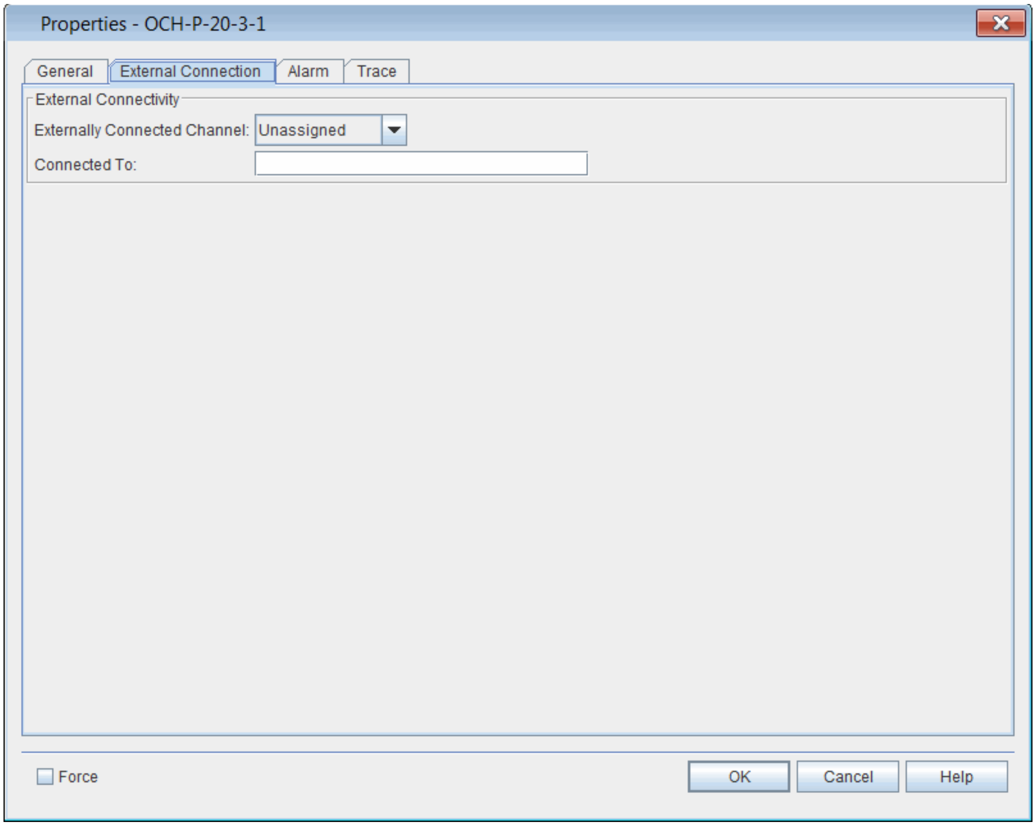
9.29 Connect an OCH-P facility on a module to another 7100 OTS/7100 Nano module or to a third-party DWDM multiplexer by performing the following steps:

__ 1. In the **Navigation Window**, expand the transponder to view the OCH-P facility.

__ 2. Right-click the **OCH-P-x-x-x** facility to view the shortcut menu, then click **Properties**. The **Properties - OCH-P-x-x-x** dialog box displays.

__ 3. Click the **External Connection** tab. Refer to Figure 9.8, page 15-186.

Figure 9.8 Properties - OCH-P-x-x-x - Enable External Connection



Properties - OCH-P-20-3-1

External Connectivity

Externally Connected Channel: Unassigned

Connected To:

□ Force

__ 4. Click the **Externally Connected Channel** drop-down box to select the channel to connect (**1**–**88**).

__ 5. Type a description of the external connection in the **Connected To** box (maximum of 36 characters).

__ 6. Click **OK**.

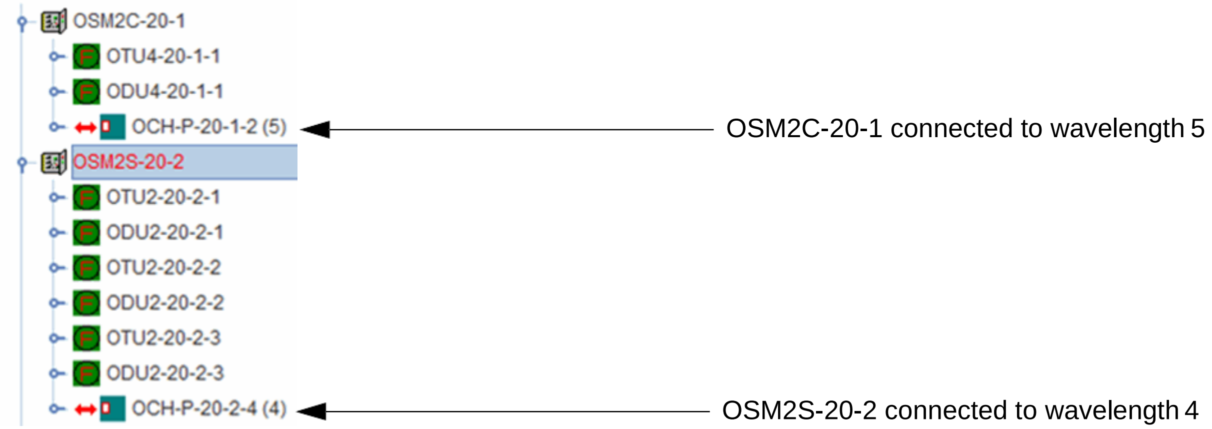
__ 7. If you are connecting to a third-party DWDM multiplexer, the procedure is complete. If you are connecting to a 7100 OTS/7100 Nano module, repeat steps 1, page 15-185 through 6, page 15-186 for the other module.

Note: *Both modules must be transmitting at the same signal rate.*

Verifying External Connection

9.30 After you configure an external connection, the channel to which the transponder is connected displays in the Navigation Window. An icon also displays next to the OCH-P facility. Refer to Figure 9.9, page 15-187.

Figure 9.9 External Connections in Navigation Window



OSM2C-20-1
OTU4-20-1-1
ODU4-20-1-1
OCH-P-20-1-2 (5)
OSM2S-20-2
OTU2-20-2-1
ODU2-20-2-1
OTU2-20-2-2
ODU2-20-2-2
OTU2-20-2-3
ODU2-20-2-3
OCH-P-20-2-4 (4)

OSM2C-20-1 connected to wavelength 5
OSM2S-20-2 connected to wavelength 4

Deleting External Connection

9.31 Delete an external connection by performing the following steps:

__ 1. In the **Navigation Window**, expand the transponder to view the OCH-P facility.

__ 2. Right-click the **OCH-P-x-x-x** facility to view the shortcut menu, then click **Properties**. The **Properties - OCH-P-x-x-x** dialog box displays.

__ 3. Click the **External Connection** tab. Refer to Figure 9.8, page 15-186.

__ 4. Click the **Externally Connected Channel** drop-down box to select **Unassigned**.

__ 5. Click **OK**.

10. Provisioning Facilities

10.1 This section contains procedures to provision facilities.

Note: *Refer to TL1 Command Reference Manual for additional details on facility parameters. Click the Help menu in the Craft Station to access this document.*

Module/Facility Support

10.2 For information about facility types supported by pluggable transceivers, refer to the Software Release Document.

10.3 Table 10.1, page 15-188 lists facility types and the modules that support each type.

Table 10.1 Facility Types and the Modules that Support Each Type

Facility Interfaces	Data Rate	OSM-2C	OSM-2S
OC192 / STM64[2]	9.953 Gbps		X
10G Ethernet LAN/10GBASE-R	10.313 Gbps		X
OTU2e[1]	11.09 Gbps		X
OTU2	10.709 Gbps		X
OCH-P	10.7 Gbps		X
OCH-P (OTU2e)	11.09 Gbps		X
100G ETH	103.125 Gbps	X	
OTU4	111.8 Gbps	X	
OCH-P[2] (OTU4v DWDM - Coherent wavelength)	120.579 Gbps	X	

[1] Transports a 10 Gigabit Ethernet local area network (LAN) PHY coming from IP/Ethernet switches and routers at full line rate (10.3 Gbps). This is specified in G.Sup43.

[2] Not supported on current version HW ready only, SW support expected to 2017 please consult Roadmap for availability information.

Creating Facilities

10.4 To provision a facility on a module, right-click the module icon in the Navigation Window, then click Create Port Facility. The Create Port Facility dialog box displays. For details about facility properties, refer to *TL1 Command Reference Manual*. Click the Help menu in the Craft Station to access this document.

10.5 Refer to the following sections for information about creating facilities:

- Optical Transport Network Facilities (OTU/ODU), page 15-189
- Ethernet Facilities, page 15-209
- SONET/SDH Facilities, page 15-213

Optical Transport Network Facilities (OTU/ODU)

10.6 OTN facilities include OTU, ODU, and OCH-P. This section includes the following examples:

- Optical Channel Transport Unit (OTU) Facilities, page 15-189
  - Creating OTU2 Facilities, page 15-189
  - Creating OTU4 Facilities, page 15-192
  - Modifying OTU Facilities, page 15-195
- Optical Data Unit (ODU) Facilities, page 15-196
  - ODU Multiplexing, page 15-199

10.7 For information about creating and managing OCH-P facilities, refer to OCH-P Facilities, page 15-205.

Optical Channel Transport Unit (OTU) Facilities

10.8 This section includes the following examples:

- Creating OTU2 Facilities, page 15-189
- Creating OTU4 Facilities, page 15-192
- Modifying OTU Facilities, page 15-195

Creating OTU2 Facilities

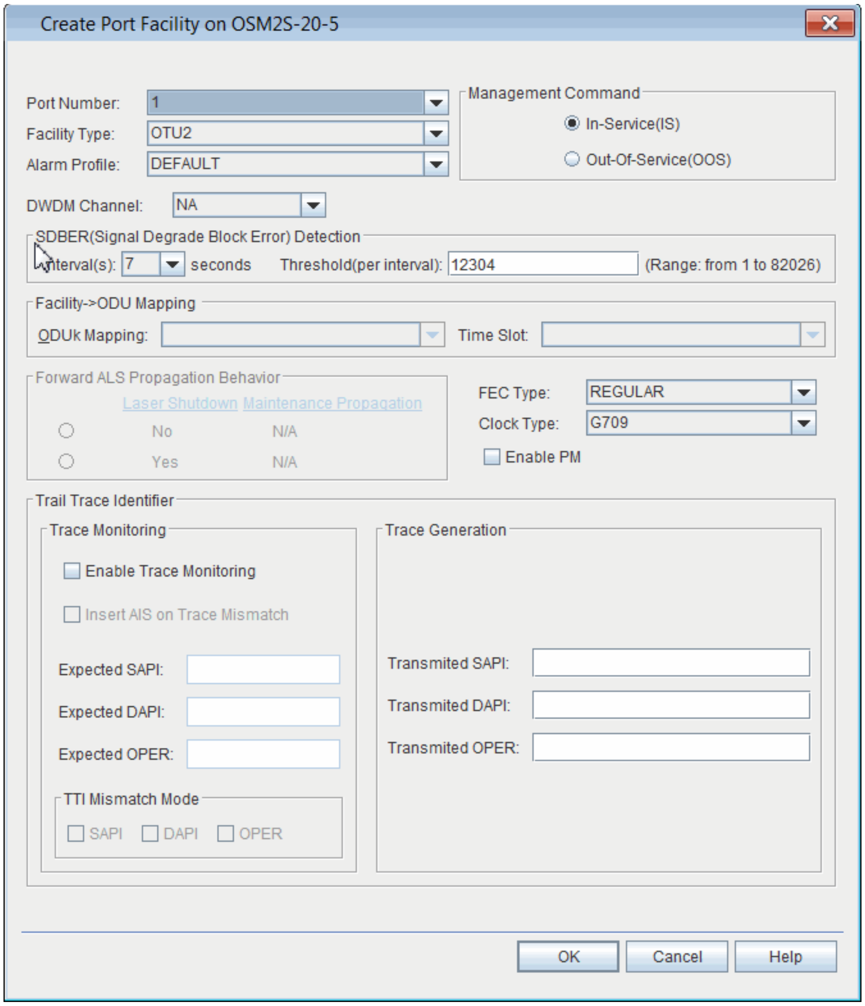
10.9 This section describes how to create an OTU2 port-side facility on an OSM-2S.

Note: *The OSM-2S supports 20 SFPP client ports. The 20 SFP client ports support the following facility types: OTU2, OCH-P, OC192, STM64, and TGLAN.*

10.10 Create an OTU2 facility on an OSM-2S by performing the following steps:

__ 1. In the **Navigation Window**, right-click the OSM-2S to view the shortcut menu, then click **Create Port Facility**. The **Create Port Facility** dialog box displays. Refer to Figure 10.1, page 15-190.

Figure 10.1 Create Port Facility on OSM-2S



Create Port Facility on OSM2S-20-5

Port Number: 1

Facility Type: OTU2

Alarm Profile: DEFAULT

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

DWDM Channel: NA

SDBER(Signal Degrade Block Error) Detection

Interval(s): 7 seconds Threshold(per interval): 12304 (Range: from 1 to 82026)

Facility->ODU Mapping

ODUk Mapping: Time Slot:

Forward ALS Propagation Behavior

Laser Shutdown Maintenance Propagation

○ No N/A

○ Yes N/A

FEC Type: REGULAR

Clock Type: G709

□ Enable PM

Trail Trace Identifier

Trace Monitoring

□ Enable Trace Monitoring

□ Insert AIS on Trace Mismatch

Expected SAPI:

Expected DAPI:

Expected OPER:

TTI Mismatch Mode

□ SAPI □ DAPI □ OPER

Trace Generation

Transmited SAPI:

Transmited DAPI:

Transmited OPER:

__ 2. Click the **Port Number** drop-down box to select the port number (**1**–**20**).

__ 3. Click the **Facility Type** drop-down box to select the type of facility to be created. This example uses an OTU2 facility. The remaining parameters in this dialog box will be active or grayed-out depending on the facility selected.

__ 4. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0**–**20**, **99**).

__ 5. Click the **DWDM Channel** drop-down box to specify the channel number corresponding to the DWDM wavelength/frequency at which the signal will be transmitted when the supporting SFPP for the OTU2 facility is a tunable DWDM SFPP (**1**–**88**, **NA**). A setting of NA allows the supporting SFPP to operate at its default wavelength.

__ 6. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 7. In the **SDBER (Signal Degrade Block Error) Detection** area, perform the following steps:

__ 7.1 Click the **Intervals** drop-down box to specify the degrade interval for the purposes of SDBER detection (**2**–**10**). The degrade interval is the consecutive number of one second intervals with the number of detected block errors exceeding the block error threshold for each of those seconds.

__ 7.2 In the **Threshold** box, type the threshold number of block errors at which a one second interval will be considered degraded for the purposes of SDBER detection (**1**–**82026**).

__ 8. Click the **FEC Type** drop-down box to select **REGULAR**, **SUPER**, or **NOFEC**.

__ 9. Click the **Clock Type** drop-down box to select **G709** or **OVRCLK_FS**.

__ 10. Performance monitoring defaults to disabled. Click the **Enable PM** check box to turn on performance monitoring functions.

__ 11. (Optional) In the **Trace Monitoring** area, configure trace monitoring by performing the following steps:

__ 11.1 Click the **Enable Trace Monitoring** box to enable trace monitoring.

__ 11.2 Click the **Insert AIS on Trace Mismatch** box to insert an alarm indication signal on trace mismatch.

__ 11.3 In the **Expected SAPI** box, type the expected source access point identifier (SAPI) text (1–15 characters).

__ 11.4 In the **Expected DAPI** box, type the expected destination access point identifier (DAPI) text (1–15 characters).

__ 11.5 In the **Expected OPER** box, type the expected operator specific trace (**OPER**) text (1–32 characters).

__ 12. (Optional) In the **Trace Generation** area, configure trace generation by performing the following steps:

__ 12.1 In the **Transmitted SAPI** box, type the source access point identifier (SAPI) text to transmit (1–15 characters).

__ 12.2 In the **Transmitted DAPI** box, type the destination access point identifier (DAPI) text to transmit (1–15 characters).

__ 12.3 In the **Transmitted OPER** box, type the operator specific trace (OPER) text to transmit (1–32 characters).

__ 13. (Optional) In the **TTI Mismatch Mode** area, configure the definition of the trail trace identifier (TTI) mismatch alarm by identifying which portions of the TTI message are compared for trace identifier mismatch purposes.

__ 13.1 Click **SAPI** to include source access point identifier mismatches in the TTI alarm.

__ 13.2 Click **DAPI** to include destination access point identifier mismatches in the TTI alarm.

__ 13.3 Click **OPER** (Operator Specific Trace) to include operator specific trace mismatches in the TTI alarm.

__ 14. Click **OK**.

Creating OTU4 Facilities

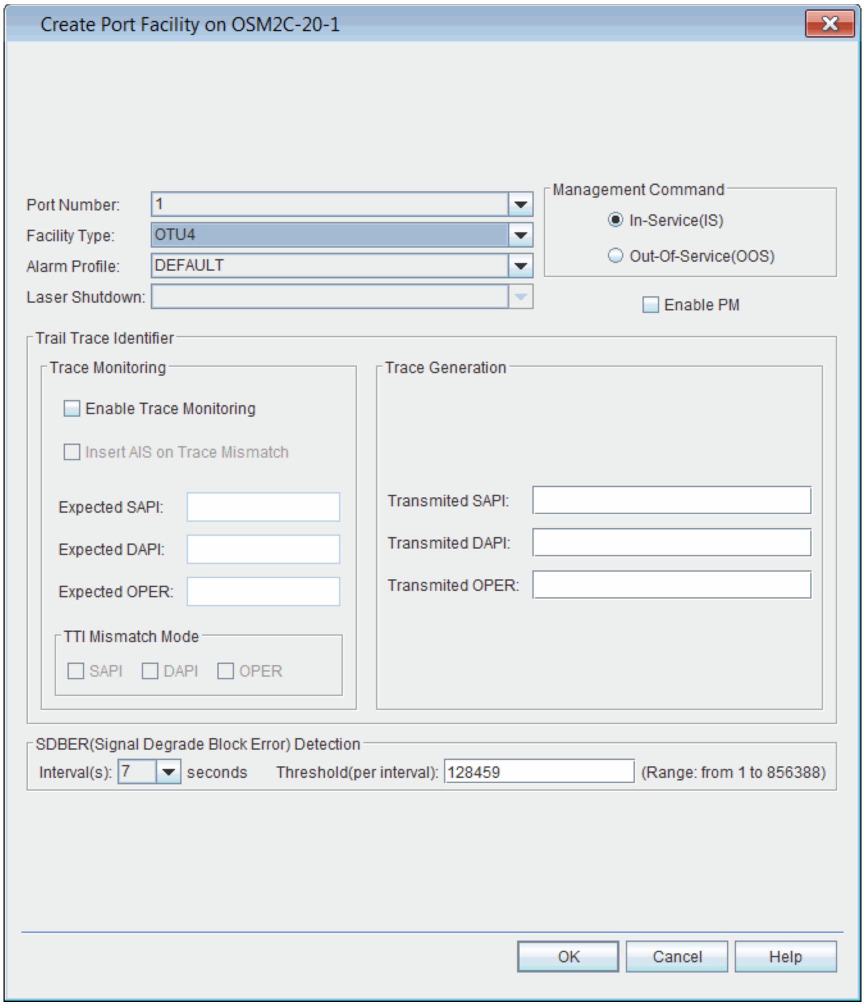
10.11 This section describes how to create an OTU4 port-side facility on an OSM-2C.

Note: *The OSM-2C supports 2 CFP client ports. The 2 CFP client ports support the following facility types: OTU4, HGE, and OCH-P.*

10.12 Provision an OTU4 port facility on an OSM-2C by performing the following steps:

__ 1. In the **Navigation Window**, right-click the transponder icon, then click **Create Port Facility**. The **Create Port Facility** dialog box displays. Refer to Figure 10.2, page 15-193.

Figure 10.2 Create Port Facility - OSM-2C Example



Create Port Facility on OSM2C-20-1

Port Number: 1

Facility Type: OTU4

Alarm Profile: DEFAULT

Laser Shutdown:

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

□ Enable PM

Trail Trace Identifier

Trace Monitoring

□ Enable Trace Monitoring

□ Insert AIS on Trace Mismatch

Expected SAPI:

Expected DAPI:

Expected OPER:

TTI Mismatch Mode

□ SAPI □ DAPI □ OPER

Trace Generation

Transmited SAPI:

Transmited DAPI:

Transmited OPER:

SDBER(Signal Degrade Block Error) Detection

Interval(s): 7 seconds Threshold(per interval): 128459 (Range: from 1 to 856388)

__ 2. Click the **Facility Type** drop-down box to select the type of facility to be created. This example uses an OTU4 facility. The remaining parameters in this dialog box will be active or grayed-out depending on the facility selected.

Note: *Refer to TL1 Command Reference Manual for additional details on facility parameters. Click the Help menu in the Craft Station to access this document.*

__ 3. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT, 0–20**, **99**).

__ 4. Click the **Enable PM** check box to activate performance monitoring for the facility.

__ 5. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 6. (Optional) In the **Trace Monitoring** area, configure trace monitoring by performing the following steps:

__ 6.1 Click the **Enable Trace Monitoring** box to enable trace monitoring.

__ 6.2 Click the **Insert AIS on Trace Mismatch** box to insert an alarm indication signal on trace mismatch.

__ 6.3 In the **Expected SAPI** box, type the expected source access point identifier (SAPI) text (1–15 characters).

__ 6.4 In the **Expected DAPI** box, type the expected destination access point identifier (DAPI) text (1–15 characters).

__ 6.5 In the **Expected OPER** box, type the expected operator specific trace (OST) text (1–32 characters).

__ 7. (Optional) In the **Trace Generation** area, configure trace generation by performing the following steps:

__ 7.1 In the **Transmitted SAPI** box, type the source access point identifier (SAPI) text to transmit (1–15 characters).

__ 7.2 In the **Transmitted DAPI** box, type the destination access point identifier (DAPI) text to transmit (1–15 characters).

__ 7.3 In the **Transmitted OPER** box, type the operator specific trace (OST) text to transmit (1–32 characters).

__ 8. (Optional) In the **TTI Mismatch Mode** area, configure the definition of the trail trace identifier (TTI) mismatch alarm by identifying which portions of the TTI message are compared for trace identifier mismatch purposes.

__ 8.1 Click **SAPI** to include source access point identifier mismatches in the TTI alarm.

__ 8.2 Click **DAPI** to include destination access point identifier mismatches in the TTI alarm.

__ 8.3 Click **OPER** (Operator Specific Trace) to include operator specific trace mismatches in the TTI alarm.

__ 9. Click the **Intervals** drop-down box to specify the degrade interval for the purposes of SDBER detection (**2**–**10**). The degrade interval is the consecutive number of one second intervals with the number of detected block errors exceeding the block error threshold for each of those seconds.

__ 10. In the **Threshold** box, type the threshold number of block errors at which a one second interval will be considered degraded for the purposes of SDBER detection (**1**–**856388**).

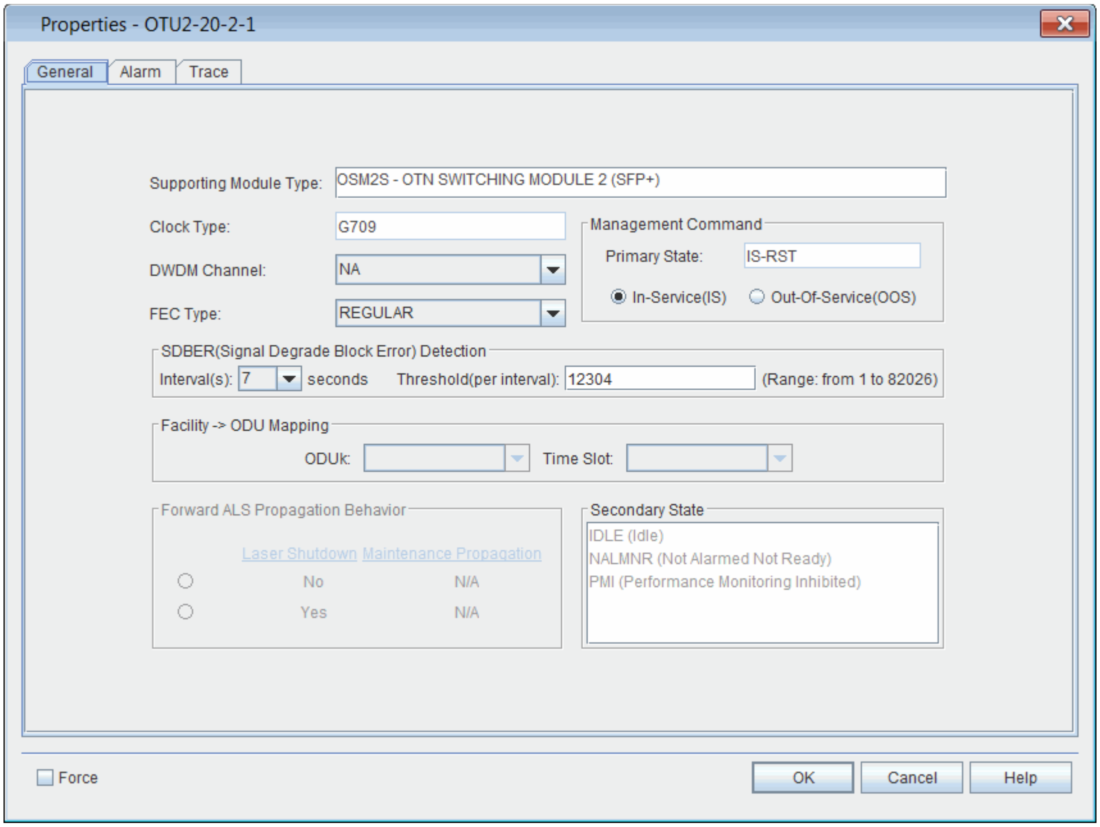
__ 11. Click **OK**.

Modifying OTU Facilities

10.13 Modify the properties of an OTU facility by performing the following steps:

__ 1. In the **Navigation Window**, expand the module icon. Right-click the **OTU** icon to view the shortcut menu, then click **Properties**. The **Properties - OTUx** dialog box displays. Refer to Figure 10.3, page 15-195 for an example of an OTU2 supported by an OSM-2S.

Figure 10.3 Properties - OTU2



Properties - OTU2-20-2-1

General | Alarm | Trace

Supporting Module Type: OSM2S - OTN SWITCHING MODULE 2 (SFP+)

Clock Type: G709

DWDM Channel: NA

FEC Type: REGULAR

Management Command

Primary State: IS-RST

● In-Service(IS) ○ Out-Of-Service(OOS)

SDBER(Signal Degrade Block Error) Detection

Interval(s): 7 seconds Threshold(per interval): 12304 (Range: from 1 to 82026)

Facility -> ODU Mapping

ODUk: Time Slot:

Forward ALS Propagation Behavior

	Laser Shutdown	Maintenance Propagation
○	No	N/A
○	Yes	N/A

Secondary State

IDLE (Idle)
NALMNR (Not Alarmed Not Ready)
PMI (Performance Monitoring Inhibited)

□ Force

__ 2. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 3. Click the **FEC Type** drop-down box to select **REGULAR**, **SUPER**, or **NOFEC**.

__ 4. In the **SDBER (Signal Degrade Block Error) Detection** area, perform the following steps:

__ 4.1 Click the **Intervals** drop-down box to specify the degrade interval for the purposes of SDBER detection (**2**–**10**). The degrade interval is the consecutive number of one second intervals with the number of detected block errors exceeding the block error threshold for each of those seconds.

__ 4.2 In the **Threshold** box, type the threshold number of block errors at which a one second interval will be considered degraded for the purposes of SDBER detection (**1**–**20421**).

__ 5. Click **OK**.

Optical Data Unit (ODU) Facilities

10.14 ODU facilities include ODU2, ODU2e, ODU1, ODU0, and ODUF. This section contains the following examples:

- Creating ODU Facilities, page 15-197
- ODU Multiplexing, page 15-199
  - Modifying ODUk Facilities, page 15-202

10.15 Refer to Table 10.2, page 15-196 for information about how the system supports the mapping of OSM-2S facility types to ODU types.

Table 10.2 Supported OSM-2S SONET/SDH/Ethernet Facility-to-ODUk Mapping

OSM-2S Facility Type	Supported ODUk Mapping Type
OC192 STM64	ODU2
TGLAN (transmap=Line_FS)	ODU2E
TGLAN (transmap=PREAMBLE)	ODU2

10.16 Refer to Figure 10.3, page 15-196 for information about how the system supports the mapping of the OTN facility (supported by the OSM-2S) to the ODU type.

Table 10.3 Supported OSM-2S OTN Facility-to-ODUk Mapping

OSM-2S Facility Type	Supported ODUk Mapping Type
OTU2/OCH-P (clktype=G709)	ODU2
OTU2/OCH-P (clktype=FS)	ODU2E

Creating ODU Facilities

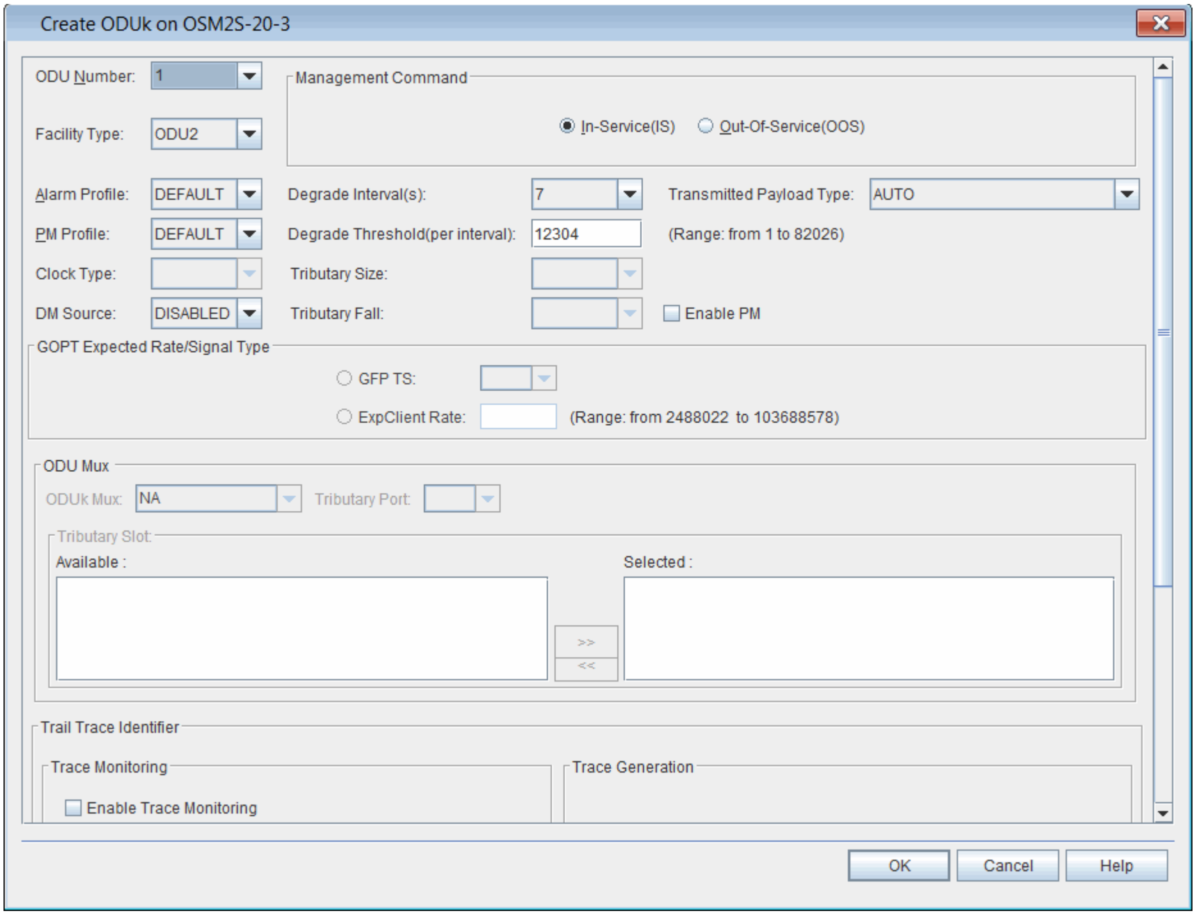
10.17 You can create ODU facilities on the following modules: OSM-2S and OSM-2C. This example describes how to create an ODU facility on an OSM-2S.

Note: *The port facility must be provisioned before the ODU facility or the creation of the ODU facility is denied.*

10.18 Create an ODU facility on an OSM-2S by performing the following steps:

__ 1. In the **Navigation Window**, right-click the ODU to view the shortcut menu, then click **Create ODUk**. The **Create ODUk on OSM2S** dialog box displays. Refer to Figure 10.4, page 15-197.

Figure 10.4 Create ODUk on ODU2 (OSM-2S Example)



Create ODUk on OSM2S-20-3

ODU Number: 1

Facility Type: ODU2

Management Command: ● In-Service(IS) ○ Out-Of-Service(OOS)

Alarm Profile: DEFAULT

PM Profile: DEFAULT

Clock Type:

DM Source: DISABLED

Degrade Interval(s): 7

Degrade Threshold(per interval): 12304 (Range: from 1 to 82026)

Tributary Size:

Tributary Fall:

Transmitted Payload Type: AUTO

□ Enable PM

GOPT Expected Rate/Signal Type

○ GFP TS:

○ ExpClient Rate: (Range: from 2488022 to 103688578)

ODU Mux

ODUk Mux: NA

Tributary Port:

Tributary Slot

Available :

Selected :

Trail Trace Identifier

Trace Monitoring

□ Enable Trace Monitoring

Trace Generation

__ 2. Click the **ODU Number** drop down box to select the ODU number.

- The OSM-2S supports ODU2 and ODU2e facilities in ports **1**–**20**.
- The OSM-2C supports ODU4 facilities in ports **1**–**2**.

__ 3. Click the **Facility Type** drop-down box to select the type of facility to be created. The remaining parameters in this dialog box will be active or grayed-out depending on the facility selected.

__ 4. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0**–**20**, **99**).

__ 5. Click the **PM Profile** drop-down box to select the default performance monitoring profile (**DEFAULT**, **0**, **1**–**20**, **99**).

__ 6. Click the **DM Source** drop-down box to select **Enabled** or **Disabled**. (Default is disabled.) DM Source specifies whether or not the entity is acting as the Source of the Delay Measurement function for performance monitoring. For an end-to-end ODUk/ODUkT path, there are two terminations and only one of the two should have DM Source set to Enabled in order to get proper delay measurement values.

__ 7. Click the **Degrade Interval** drop-down box to specify the degrade interval for the purposes of SDBER detection (**2**–**10**). The degrade interval is the consecutive number of one second intervals with the number of detected block errors exceeding the block error threshold for each of those seconds.

__ 8. Click the **Degrade Threshold** drop-down box to specify the threshold number of block errors at which a one second interval will be considered degraded for the purposes of SDBER detection (**1**–**82026** for ODU2, **1**–**84986** for ODU2e, **1**–**856388** for ODU4).

__ 9. Performance monitoring defaults to disabled. Click the **Enable PM** check box to turn on performance monitoring functions.

__ 10. In the **GOPT Expected Rate/Signal Type** area, choose one of the following options:

- In the **ExpClient Rate** box, type the expected signal rate (2488022 Kbps–103688578 Kbps). The signal rate will be one of the following:
  - expected signal rate on the GOPT facility or range on the specified GOPT facility to be mapped to the ODUF
  - if the non-terminated ODUF is an ODUF (CBR), then set rate based on the expected client rate of the signal being carried within the ODUF.
- If the non-terminated ODUF is an ODUF (GFP), then click the **GFP TS** box and specify an integer number of tributary slots (1.25 G) worth of GFP bandwidth.

__ 11. Click the **ODU Mux** drop-down box to select the facility on which to mux the ODUk that you are creating.

__ 12. Click the **Tributary Port** drop-down box to select **1** or **2**.

__ 13. In the **Tributary Slot** area, select the tributaries to map to the ODU. Click to highlight the facility in the **Available** list, and move it to the **Selected** list by clicking the right-facing arrow.

__ 14. (Optional) In the **Trace Monitoring** area, configure trace monitoring by performing the following steps:

__ 14.1 Click the **Enable Trace Monitoring** box to enable trace monitoring.

__ 14.2 Click the **Insert AIS on Trace Mismatch** box to insert an alarm indication signal on trace mismatch.

__ 14.3 In the **Expected SAPI** box, type the expected source access point identifier (SAPI) text (1–15 characters).

__ 14.4 In the **Expected DAPI** box, type the expected destination access point identifier (DAPI) text (1–15 characters).

__ 14.5 In the **Expected OPER** box, type the expected operator specific trace (OPER) text (1–32 characters).

__ 15. (Optional) In the **Trace Generation** area, configure trace generation by performing the following steps:

__ 15.1 In the **Transmitted SAPI** box, type the source access point identifier (SAPI) text to transmit (1–15 characters).

__ 15.2 In the **Transmitted DAPI** box, type the destination access point identifier (DAPI) text to transmit (1–15 characters).

__ 15.3 In the **Transmitted OPER** box, type the operator specific trace (OPER) text to transmit (1–32 characters).

__ 16. (Optional) In the **TTI Mismatch Mode** area, configure the definition of the trail trace identifier (TTI) mismatch alarm by identifying which portions of the TTI message are compared for trace identifier mismatch purposes.

__ 16.1 Click **SAPI** to include source access point identifier mismatches in the TTI alarm.

__ 16.2 Click **DAPI** to include destination access point identifier mismatches in the TTI alarm.

__ 16.3 Click **OPER** (Operator Specific Trace) to include operator specific trace mismatches in the TTI alarm.

__ 17. In the **Management Command** area, click **In-Service (IS)** or **Out-Of-Service(OOS)**.

__ 18. Click **OK**.

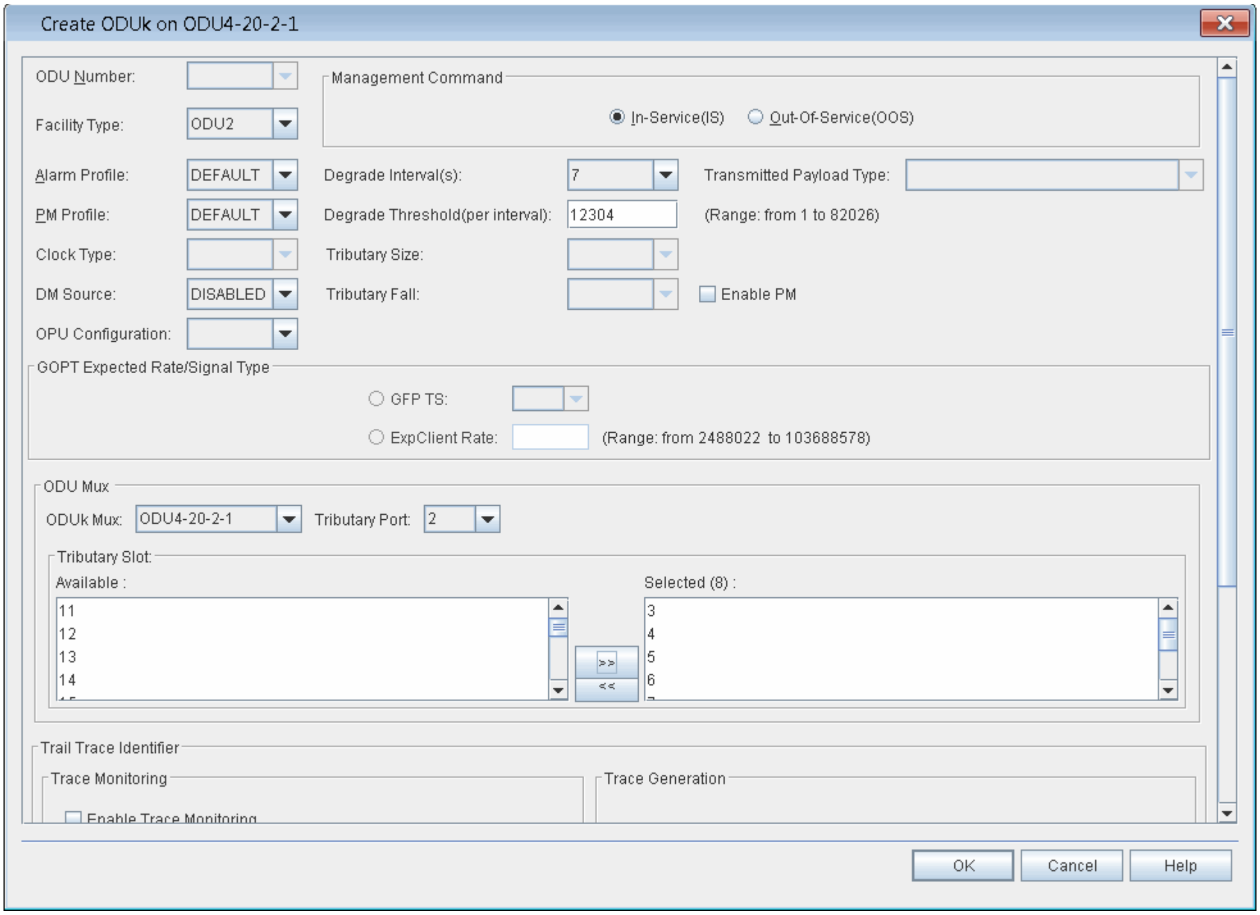
ODU Multiplexing

10.19 The OSM-2C supports two-stage ODU multiplexing. This example describes how to multiplex an ODU2 into an ODU4 facility.

__ 1. In the **Navigation Window**, click to expand the facilities supported by the OSM-2C.

__ 2. Right-click the **ODU4** to view the shortcut menu, then click **Create ODUk**. The **Create ODU on ODU4** dialog box displays. Refer to Figure 10.5, page 15-200.

Figure 10.5 Create ODU2 on ODU4 (OSM-2C Example)



Create ODUk on ODU4-20-2-1

ODU Number:

Facility Type: ODU2

Alarm Profile: DEFAULT

PM Profile: DEFAULT

Clock Type:

DM Source: DISABLED

OPU Configuration:

Management Command

● In-Service(IS) ○ Out-Of-Service(OOS)

Degrade Interval(s): 7

Degrade Threshold(per interval): 12304 (Range: from 1 to 82026)

Transmitted Payload Type:

Tributary Size:

Tributary Fall:

□ Enable PM

GOPT Expected Rate/Signal Type

○ GFP TS:

○ ExpClient Rate: (Range: from 2488022 to 103688578)

ODU Mux

ODUk Mux: ODU4-20-2-1 Tributary Port: 2

Tributary Slot:

Available : 11 12 13 14

Selected (8) : 3 4 5 6

Trail Trace Identifier

Trace Monitoring

□ Enable Trace Monitoring

Trace Generation

__ 3. Click the **Facility Type** drop-down box to select the type of facility to be created. The remaining parameters in this dialog box will be active or grayed-out depending on the facility selected. This example uses an ODU2.

__ 4. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0**–**20**, **99**).

__ 5. Click the **PM Profile** drop-down box to select the default performance monitoring profile (**DEFAULT**, **0**, **1**–**20**, **99**).

__ 6. Click the **DM Source** drop-down box to select **Enabled** or **Disabled**. (Default is disabled.) DM Source specifies whether or not the entity is acting as the Source of the Delay Measurement function for performance monitoring. For an end-to-end ODUk/ODUkT path, there are two terminations and only one of the two should have DM Source set to Enabled in order to get proper delay measurement values.

__ 7. Click the **Degrade Interval** drop-down box to specify the degrade interval for the purposes of SDBER detection (**2**–**10**). The degrade interval is the consecutive number of one second intervals with the number of detected block errors exceeding the block error threshold for each of those seconds.

__ 8. Click the **Degrade Threshold** drop-down box to specify the threshold number of block errors at which a one second interval will be considered degraded for the purposes of SDBER detection (**1-20516** for ODUF and **1-20421** for ODU1, **1-10168** for ODU0).

__ 9. Performance monitoring defaults to disabled. Click the **Enable PM** check box to turn on performance monitoring functions.

__ 10. In the **GOPT Expected Rate/Signal Type** area, choose one of the following options:

- In the **ExpClient Rate** box, type the expected signal rate (2488022 Kbps–9952261 Kbps). The signal rate will be one of the following:
    - expected signal rate on the GOPT facility or range on the specified GOPT facility to be mapped to the ODUF
    - if the non-terminated ODUF is an ODUF (CBR), then set rate based on the expected client rate of the signal being carried within the ODUF.
- If the non-terminated ODUF is an ODUF (GFP), then click the **GFP TS** box and specify an integer number of tributary slots (1.25 G) worth of GFP bandwidth.

__ 11. Click the **ODU Mux** drop-down box to select the facility on which to mux the ODUk that you are creating.

__ 12. In the **Tributary Slot** area, select the tributaries to map to the ODU. Click to highlight the facility in the **Available** list, and move it to the **Selected** list by clicking the right-facing arrow.

__ 13. (Optional) In the **Trace Monitoring** area, configure trace monitoring by performing the following steps:

__ 13.1 Click the **Enable Trace Monitoring** box to enable trace monitoring.

__ 13.2 Click the **Insert AIS on Trace Mismatch** box to insert an alarm indication signal on trace mismatch.

__ 13.3 In the **Expected SAPI** box, type the expected source access point identifier (SAPI) text (1–15 characters).

__ 13.4 In the **Expected DAPI** box, type the expected destination access point identifier (DAPI) text (1–15 characters).

__ 13.5 In the **Expected OPER** box, type the expected operator specific trace (OPER) text (1–32 characters).

__ 14. (Optional) In the **Trace Generation** area, configure trace generation by performing the following steps:

  __ 14.1 In the **Transmitted SAPI** box, type the source access point identifier (SAPI) text to transmit (1–15 characters).

  __ 14.2 In the **Transmitted DAPI** box, type the destination access point identifier (DAPI) text to transmit (1–15 characters).

  __ 14.3 In the **Transmitted OPER** box, type the operator specific trace (OPER) text to transmit (1–32 characters).

__ 15. (Optional) In the **TTI Mismatch Mode** area, configure the definition of the trail trace identifier (TTI) mismatch alarm by identifying which portions of the TTI message are compared for trace identifier mismatch purposes.

  __ 15.1 Click **SAPI** to include source access point identifier mismatches in the TTI alarm.

  __ 15.2 Click **DAPI** to include destination access point identifier mismatches in the TTI alarm.

  __ 15.3 Click **OPER** (Operator Specific Trace) to include operator specific trace mismatches in the TTI alarm.

__ 16. In the **Management Command** area, click **In-Service (IS)** or **Out-Of-Service(OOS)**.

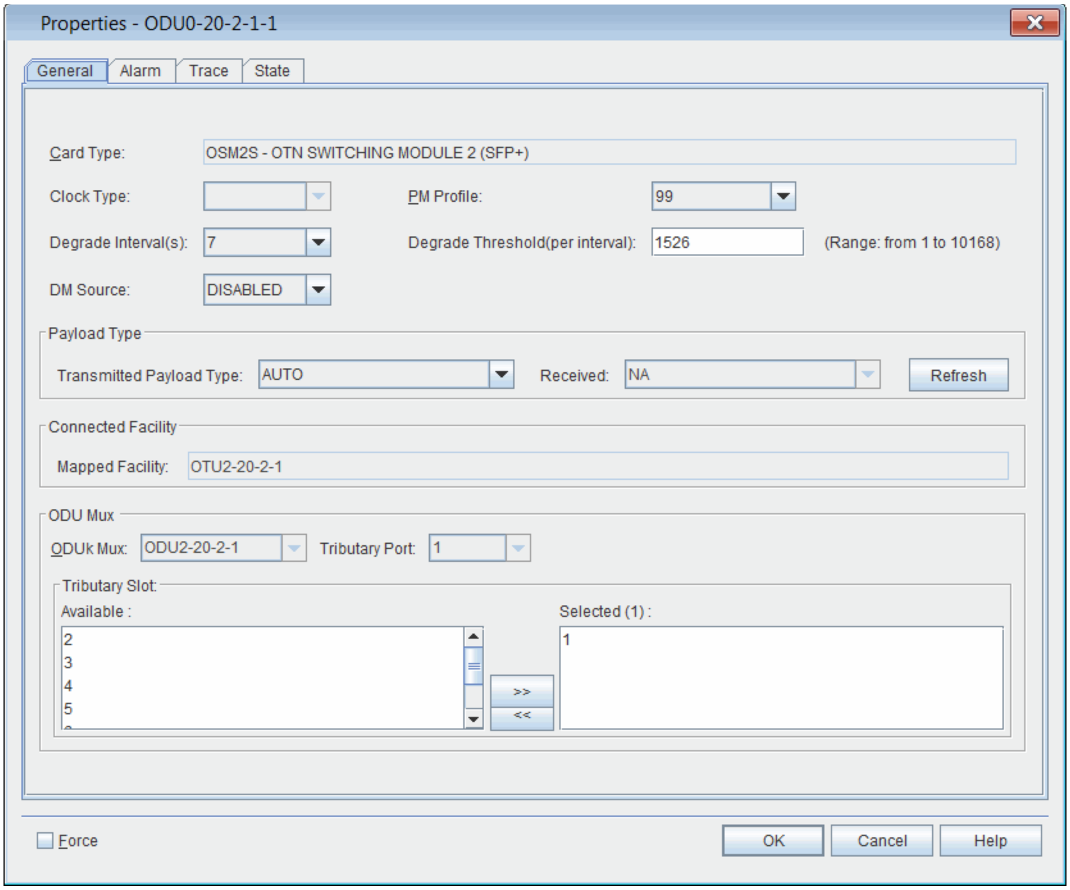
__ 17. Click **OK**.

Modifying ODUk Facilities

10.20 View or modify the properties of an ODUk facility by performing the following steps:

__ 1. In the **Navigation Window**, right-click the ODUk facility to view the shortcut menu, then click **Properties**. The **Properties - ODUk** dialog box displays. Refer to Figure 10.6, page 15-203.

Figure 10.6 Properties - ODU0



Properties - ODU0-20-2-1-1

Card Type: OSM2S - OTN SWITCHING MODULE 2 (SFP+)

Clock Type:

PM Profile: 99

Degrade Interval(s): 7

Degrade Threshold(per interval): 1526 (Range: from 1 to 10168)

DM Source: DISABLED

Payload Type

Transmitted Payload Type: AUTO

Received: NA

Connected Facility

Mapped Facility: OTU2-20-2-1

ODU Mux

ODUk Mux: ODU2-20-2-1

Tributary Port: 1

Tributary Slot

Available :
2
3
4
5

Selected (1) :
1

☐ Force

General Tab

__ 2. Verify that the **General** tab is selected.

__ 3. Click the **PM Profile** drop-down box to select the default performance monitoring profile (**DEFAULT**, **0**, **1**–**20**, **99**).

__ 4. Click the **Degrade Interval** drop-down box to specify the degrade interval for the purposes of SDBER detection (**2**–**10**). The degrade interval is the consecutive number of one second intervals with the number of detected block errors exceeding the block error threshold for each of those seconds.

__ 5. Click the **Degrade Threshold** drop-down box to specify the threshold number of block errors at which a one second interval will be considered degraded for the purposes of SDBER detection (**1**–**10168**).

__ 6. Click the **DM Source** drop-down box to select **Enabled** or **Disabled**. (Default is disabled.) DM Source specifies whether or not the entity is acting as the Source of the Delay Measurement function for performance monitoring. For an end-to-end ODUk/ODUkT path, there are two terminations and only one of the two should have DM Source set to Enabled in order to get proper delay measurement values.

Alarm Tab

__ 7. Click the **Alarm Tab**.

__ 8. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0**–**20**, **99**).

__ 9. In the **Alarm List**, view any alarms posted against the facility.

Trace Tab

_ 10. Click the **Trace Tab**.

__ 11. (Optional) In the **Trace Monitoring** area, configure trace monitoring by performing the following steps:

__ 11.1 Click the **Enable Trace Monitoring** box to enable trace monitoring.

__ 11.2 Click the **Insert AIS on Trace Mismatch** box to insert an alarm indication signal on trace mismatch.

__ 11.3 In the **Expected SAPI** box, type the expected source access point identifier (SAPI) text (1–15 characters).

__ 11.4 In the **Expected DAPI** box, type the expected destination access point identifier (DAPI) text (1–15 characters).

__ 11.5 In the **Expected OPER** box, type the expected operator specific trace (OPER) text (1–32 characters).

__ 12. (Optional) In the **Trace Generation** area, configure trace generation by performing the following steps:

__ 12.1 In the **Transmitted SAPI** box, type the source access point identifier (SAPI) text to transmit (1–15 characters).

__ 12.2 In the **Transmitted DAPI** box, type the destination access point identifier (DAPI) text to transmit (1–15 characters).

__ 12.3 In the **Transmitted OPER** box, type the operator specific trace (OPER) text to transmit (1–32 characters).

__ 13. (Optional) In the **TTI Mismatch Mode** area, configure the definition of the trail trace identifier (TTI) mismatch alarm by identifying which portions of the TTI message are compared for trace identifier mismatch purposes.

__ 13.1 Click **SAPI** to include source access point identifier mismatches in the TTI alarm.

__ 13.2 Click **DAPI** to include destination access point identifier mismatches in the TTI alarm.

__ 13.3 Click **OPER** (Operator Specific Trace) to include operator specific trace mismatches in the TTI alarm.

State Tab

_ 14. Click the **State** tab.

__ 15. In the **Management Command** area, click **In-Service (IS)** or **Out-Of-Service(OOS)**.

__ 16. In the **Command Mode** area, click **Forced** or **Normal**.

__ 17. Click **OK**.

OCH-P Facilities

10.21 OCH-P facilities are also considered to be part of the OTN layer. In the 7100 OTS/7100 Nano system, OCH-P interfaces are OTUk signals that additionally have the OCh layer with the wavelength settings and information.

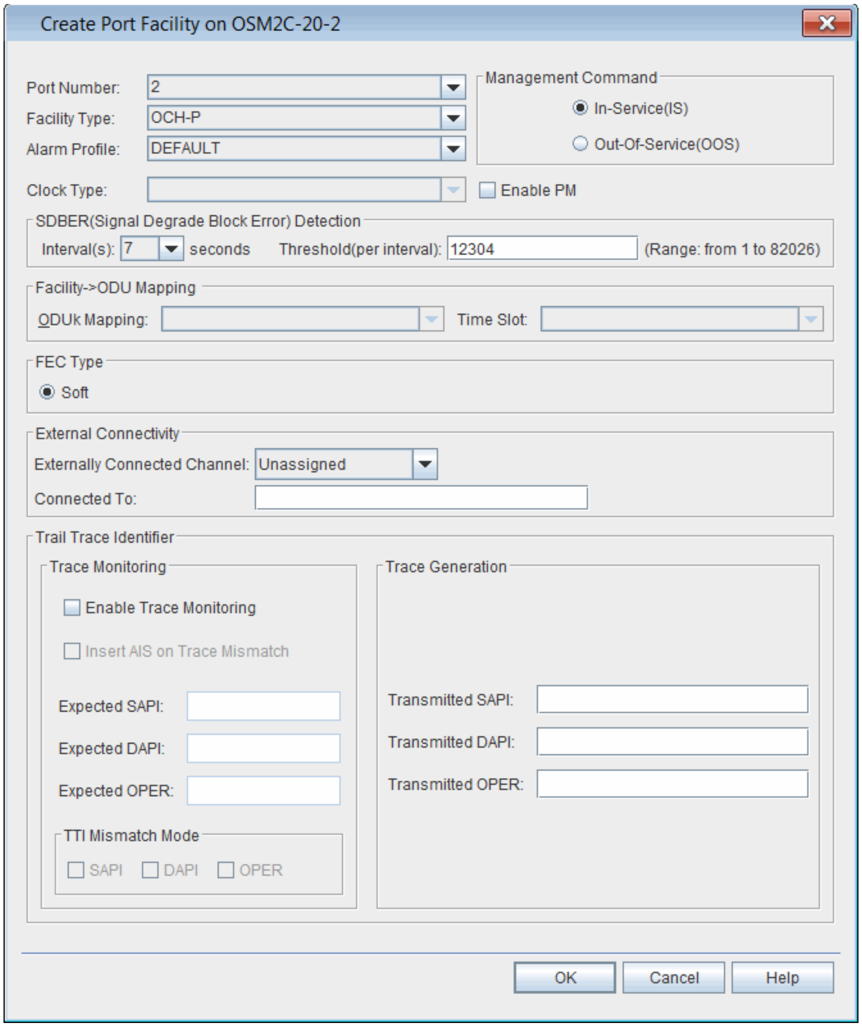
OCH-P

10.22 This section provides an example of how to create an OCH-P facility on an OSM-2C.

10.23 Create an OCH-P on the port side of an OSM-2C by performing the following steps:

__ 1. In the **Navigation Window**, right-click the OSM-2C to view the shortcut menu, then click **Create Port Facility**. The **Create Port Facility** dialog box displays. Refer to Figure 10.7, page 15-205.

Figure 10.7 Create Port Facility on OSM-2C



Create Port Facility on OSM2C-20-2

Port Number: 2

Facility Type: OCH-P

Alarm Profile: DEFAULT

Clock Type:

Management Command: ● In-Service(IS) ○ Out-Of-Service(OOS)

□ Enable PM

SDBER(Signal Degrade Block Error) Detection: Interval(s): 7 seconds Threshold(per interval): 12304 (Range: from 1 to 82026)

Facility->ODU Mapping: ODUk Mapping: Time Slot:

FEC Type: ● Soft

External Connectivity: Externally Connected Channel: Unassigned Connected To:

Trail Trace Identifier

Trace Monitoring: □ Enable Trace Monitoring □ Insert AIS on Trace Mismatch

Expected SAPI:

Expected DAPI:

Expected OPER:

TTI Mismatch Mode: □ SAPI □ DAPI □ OPER

Trace Generation: Transmitted SAPI: Transmitted DAPI: Transmitted OPER:

__ 2. Click the **Port Number** drop-down box to select an available port (**1–2**).

__ 3. Click the **Facility Type** drop-down box to select the facility type. This example uses an OCH-P facility. The remaining parameters in this dialog box will be active or grayed-out depending on the facility selected.

__ 4. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT, 0**–**20**, **99**).

__ 5. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 6. (Optional) Click the **Externally Connected Channel** drop-down box to select the channel to which this OCH-P will be externally connected (**1**–**88**).

__ 7. (Optional) In the **Connected To** box, type a description of the external connection.

__ 8. (Optional) In the **Trace Monitoring** area, configure trace monitoring by performing the following steps:

__ 8.1 Click the **Enable Trace Monitoring** box to enable trace monitoring.

__ 8.2 Click the **Insert AIS on Trace Mismatch** box to insert an alarm indication signal on trace mismatch.

__ 8.3 In the **Expected SAPI** box, type the expected source access point identifier (SAPI) text (1–15 characters).

__ 8.4 In the **Expected DAPI** box, type the expected destination access point identifier (DAPI) text (1–15 characters).

__ 8.5 In the **Expected OST** box, type the expected operator specific trace (OST) text (1–32 characters).

__ 9. (Optional) In the **Trace Generation** area, configure trace generation by performing the following steps:

__ 9.1 In the **Transmitted SAPI** box, type the source access point identifier (SAPI) text to transmit (1–15 characters).

__ 9.2 In the **Transmitted DAPI** box, type the destination access point identifier (DAPI) text to transmit (1–15 characters).

__ 9.3 In the **Transmitted OST** box, type the operator specific trace (OST) text to transmit (1–32 characters).

__ 10. (Optional) In the **TTI Mismatch Mode** area, configure the definition of the trail trace identifier (TTI) mismatch alarm by identifying which portions of the TTI message are compared for trace identifier mismatch purposes.

__ 10.1 Click **SAPI** to include source access point identifier mismatches in the TTI alarm.

__ 10.2 Click **DAPI** to include destination access point identifier mismatches in the TTI alarm.

__ 10.3 Click **OST** (Operator Specific Trace) to include operator specific trace mismatches in the TTI alarm.

__ 11. Click **OK**.

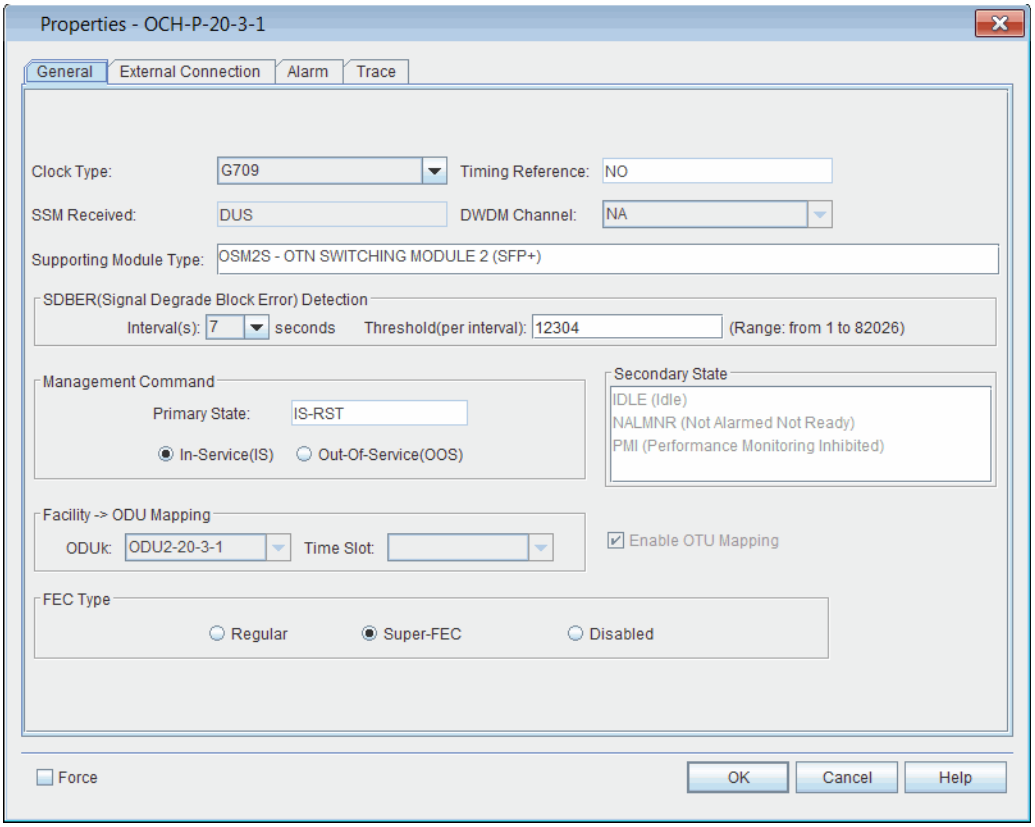
Viewing or Modifying OCH-P Properties

10.24 View or modify the parameters of an OCH-P facility by performing the following steps:

__ 1. In the **Navigation Window**, right-click the facility to view the shortcut menu, then click **Properties**. The **Properties - OCH-P** dialog box displays.

- Refer to Figure 10.8, page 15-207 to view an example of the OCH-P dialog box when the supporting module is an OSM-2S.

Figure 10.8 OCH-P Properties (OSM-2S)



Properties - OCH-P-20-3-1

Clock Type: G709
Timing Reference: NO
SSM Received: DUS
DWDM Channel: NA
Supporting Module Type: OSM2S - OTN SWITCHING MODULE 2 (SFP+)

SDBER(Signal Degrade Block Error) Detection
Interval(s): 7 seconds Threshold(per interval): 12304 (Range: from 1 to 82026)

Management Command
Primary State: IS-RST
● In-Service(IS) ○ Out-Of-Service(OOS)

Secondary State
IDLE (Idle)
NALMNR (Not Alarmed Not Ready)
PMI (Performance Monitoring Inhibited)

Facility -> ODU Mapping
ODUk: ODU2-20-3-1 Time Slot:

☑ Enable OTU Mapping

FEC Type
○ Regular ● Super-FEC ○ Disabled

□ Force

__ 2. Click the **Intervals** drop-down box to specify the degrade interval for the purposes of SDBER detection (**2**–**10**). The degrade interval is the consecutive number of one second intervals with the number of detected block errors exceeding the block error threshold for each of those seconds.

__ 3. In the **Threshold** box, type the threshold number of block errors at which a one second interval will be considered degraded for the purposes of SDBER detection (**1**–**82026**).

__ 4. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 5. In the **FEC Type** area, click **REGULAR**, **SUPER**, or **Disabled**.

External Connection Tab

__ 6. Click the **External Connection** tab.

__ 7. View information about an externally connected facility. Refer to External Connections (Direct Connect), page 15-276 for more information.

Alarm Tab

__ 8. Click the **Alarm** tab.

__ 9. View any alarms that may exist on the facility. Refer to Alarm Reporting Control, page 15-168 for information about alarm profile and ARC parameters.

Trace Tab

_ 10. Click the Trace tab.

__ 11. (Optional) In the **Trace Monitoring** area, configure trace monitoring by performing the following steps:

__ 11.1 Click the **Enable Trace Monitoring** box to enable trace monitoring.

__ 11.2 Click the **Insert AIS on Trace Mismatch** box to insert an alarm indication signal on trace mismatch.

__ 11.3 In the **Expected SAPI** box, type the expected source access point identifier (SAPI) text (1–15 characters).

__ 11.4 In the **Expected DAPI** box, type the expected destination access point identifier (DAPI) text (1–15 characters).

__ 11.5 In the **Expected OPER** box, type the expected operator specific trace (OPER) text (1–32 characters).

__ 12. (Optional) In the **Trace Generation** area, configure trace generation by performing the following steps:

__ 12.1 In the **Transmitted SAPI** box, type the source access point identifier (SAPI) text to transmit (1–15 characters).

__ 12.2 In the **Transmitted DAPI** box, type the destination access point identifier (DAPI) text to transmit (1–15 characters).

__ 12.3 In the **Transmitted OPER** box, type the operator specific trace (OST) text to transmit (1–32 characters).

__ 13. (Optional) In the **TTI Mismatch Mode** area, configure the definition of the trail trace identifier (TTI) mismatch alarm by identifying which portions of the TTI message are compared for trace identifier mismatch purposes.

__ 13.1 Click **SAPI** to include source access point identifier mismatches in the TTI alarm.

__ 13.2 Click **DAPI** to include destination access point identifier mismatches in the TTI alarm.

__ 13.3 Click **OPER** (Operator Specific Trace) to include operator specific trace mismatches in the TTI alarm.

__ 14. If trace monitoring is enabled, click **Query Trace** to display the **Received SAPI**, **Received DAPI**, and **Received OPER** in the **Trace Received** area.

__ 15. Click **OK**.

Ethernet Facilities

10.25 Ethernet facilities include HGE and TGLAN.

10.26 Refer to the following sections:

- Creating TGLAN Facilities, page 15-209
- Creating HGE Facilities, page 15-211

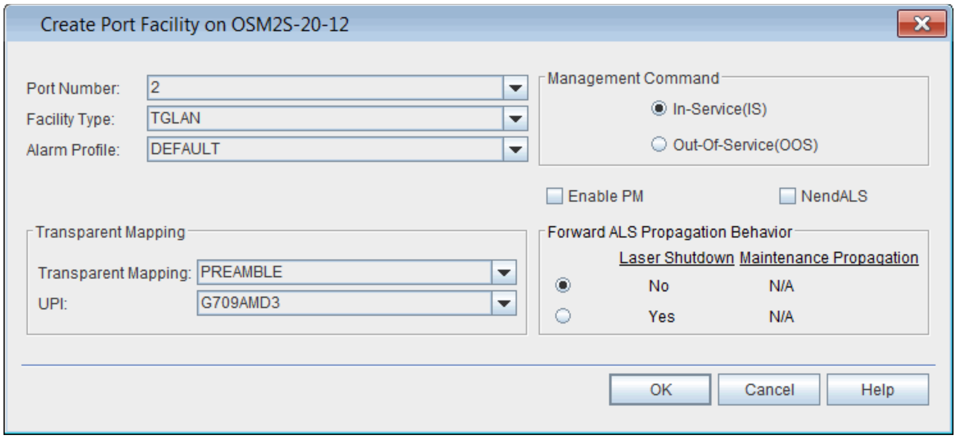
Creating TGLAN Facilities

10.27 This section provides an example of how to create a TGLAN facility on an OSM-2S.

10.28 Create a TGLAN facility by performing the following steps:

__ 1. In the **Navigation Window**, right-click the transponder icon, then click **Create Port Facility**. The **Create Port Facility** dialog box displays. Refer to Figure 10.9, page 15-210.

Figure 10.9 Create Port Facility - TGLAN Example



Create Port Facility on OSM2S-20-12

Port Number:	2
Facility Type:	TGLAN
Alarm Profile:	DEFAULT

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

□ Enable PM □ NendALS

Transparent Mapping

Transparent Mapping:	PREAMBLE
UPI:	G709AMD3

Forward ALS Propagation Behavior

	Laser Shutdown	Maintenance Propagation
●	No	N/A
○	Yes	N/A

__ 2. Click the **Type** drop-down box to select the type of facility to be created. This example uses a TGBEP facility. The remaining parameters in this dialog box will be active or grayed-out depending on the facility selected.

Note: *Refer to TL1 Command Reference Manual for additional details on facility parameters. Click the Help menu in the Craft Station to access this document.*

__ 3. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT, 0–20**, **99**).

__ 4. Click the **Transparent Mapping** drop-down box to select **PREAMBLE** or **LINE_FS**. If you set the parameter to PREAMBLE, go to step 5, page 15-210. Otherwise, go to step 6, page 15-210.

__ 5. Click the **UPI** drop-down box to configure the use payload indicator for 10 Gbps Ethernet clients. Select **GSUPP43** for compatibility with ITUT Supplemental 43 recommendation support prior to G709 amendment 3, or **G709AMD3** for compatibility with ITUT G.709 recommendation values.

__ 6. Click the **Enable PM** check box to activate performance monitoring for the facility.

__ 7. Click the **NendALS** check box to enable near end automatic laser shutdown. This parameter, when enabled, will shut down the port-side laser upon a incoming port-side failure (such as LOS, LOF, or LOSYNC).

__ 8. In the **Forward (ALS) Propagation Behavior** area, select the appropriate laser shutdown (**No**, **Yes**) and maintenance propagation behavior (**NA**). This parameter allows you to propagate maintenance signals through the network to provide the Automatic Laser Shutdown (ALS) capability without generating alarms within the network.

__ 9. In the **Management Command** area, the current state of the facility displays in the **Primary State** box. Click **In-Service(IS)** or **Out-Of-Service(OOS)** to change the state of the facility.

__ 10. Click **OK**.

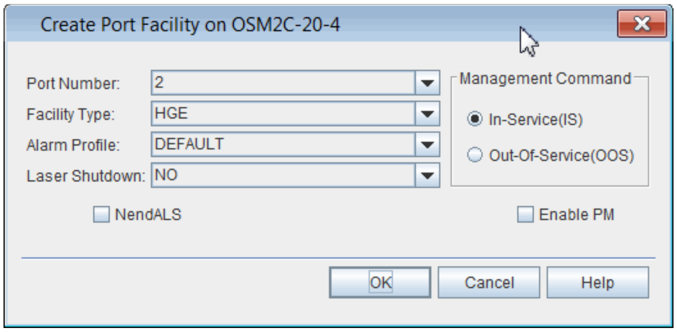
Creating HGE Facilities

10.29 This section provides an example of how to create an HGE facility on an OSM-2C.

10.30 Create an HGE facility by performing the following steps:

__ 1. In the **Navigation Window**, right-click the transponder icon, then click **Create Port Facility**. The **Create Port Facility** dialog box displays. Refer to Figure 10.10, page 15-211.

Figure 10.10 Create Port Facility - HGE Example



Create Port Facility on OSM2C-20-4

Port Number: 2

Facility Type: HGE

Alarm Profile: DEFAULT

Laser Shutdown: NO

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

□ NendALS

□ Enable PM

__ 2. Click the **Port Number** drop-down box to select the port number (**1**–**2**). This is the port number on the HGE that the facility interfaces.

__ 3. Click the **Facility Type** drop-down box to select the facility type. This example uses an HGE facility. The remaining parameters in this dialog box will be active or grayed-out depending on the facility selected.

Note: *Refer to TL1 Command Reference Manual for additional details on facility parameters. Click the Help menu in the Craft Station to access this document.*

__ 4. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0**–**20**, **99**). (The default alarm profile is the default alarm profile specified at the NE level.)

__ 5. Click the **NendALS** check box to enable near end automatic laser shutdown. This parameter, when enabled, will shut down the port-side laser upon a incoming port-side failure (such as LOS, LOF, or LOSYNC).

__ 6. Click the **Enable PM** check box to activate performance monitoring for the facility.

__ 7. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 8. Click the **Laser Shutdown** drop-down box and select the appropriate laser shutdown (**NO**, **YES**).

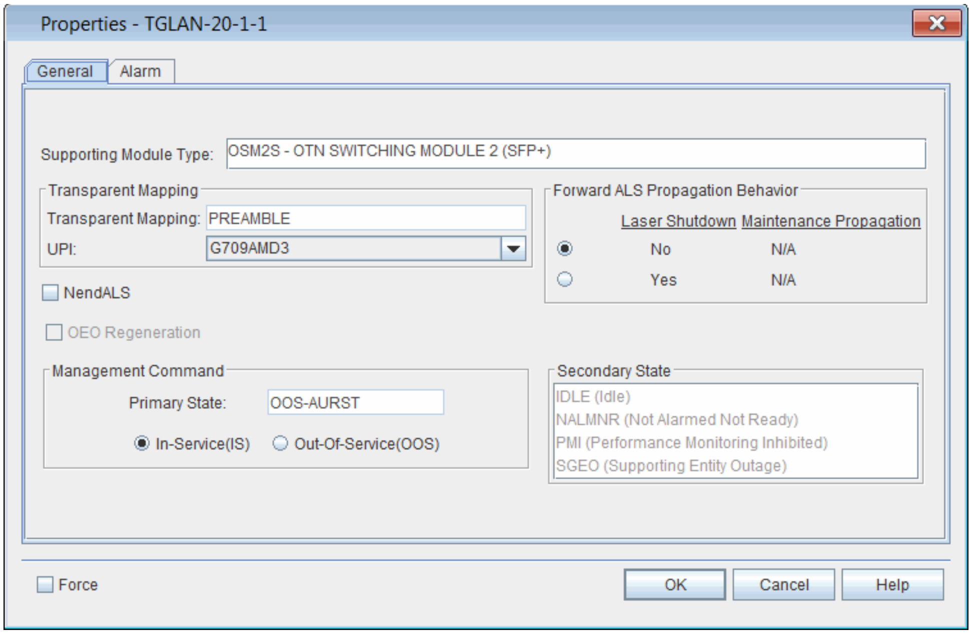
__ 9. Click **OK**.

Modifying TGLAN Properties

10.31 Modify the properties of an TGLAN facility by performing the following steps:

__ 1. In the **Navigation Window**, expand the module icon. Right-click **TGLAN** to view the shortcut menu, then click **Properties**. The **Properties - TGLAN** dialog box displays. Refer to Figure 10.11, page 15-212 for an example of an TGLAN supported by an OSM-2S.

Figure 10.11 Properties - TGLAN



Properties - TGLAN-20-1-1

Supporting Module Type: OSM2S - OTN SWITCHING MODULE 2 (SFP+)

Transparent Mapping

Transparent Mapping: PREAMBLE

UPI: G709AMD3

□ NendALS

□ OEO Regeneration

Forward ALS Propagation Behavior

	Laser Shutdown	Maintenance Propagation
●	No	N/A
○	Yes	N/A

Management Command

Primary State: OOS-AURST

● In-Service(IS) ○ Out-Of-Service(OOS)

Secondary State

IDLE (Idle)
NALMNR (Not Alarmed Not Ready)
PMI (Performance Monitoring Inhibited)
SGEO (Supporting Entity Outage)

□ Force

__ 2. Click the **GFP UPI** drop-down box to configure the use payload indicator for 10 Gbps Ethernet clients. Select **GSUPP43** for compatibility with ITUT Supplemental 43 recommendation support prior to G709 amendment 3, or **G709AMD3** for compatibility with ITUT G.709 recommendation values.

__ 3. Click the **NendALS** check box to allow port-side later shutdown on the detection of a port-side defect.

__ 4. In the **Forward (ALS) Propagation Behavior** area, select the appropriate laser shutdown (**No**, **Yes**) and maintenance propagation behavior (**NA**). This parameter allows you to propagate maintenance signals through the network to provide the Automatic Laser Shutdown (ALS) capability without generating alarms within the network.

__ 5. In the **Management Command** area, the current state of the facility displays in the **Primary State** box. Click **In-Service(IS)** or **Out-Of-Service(OOS)** to change the state of the facility.

__ 6. Click **OK**.

SONET/SDH Facilities

10.32 This section provides the following examples:

- Creating OC192/STM64, page 15-213
- Modifying OCn/STMn Properties, page 15-214

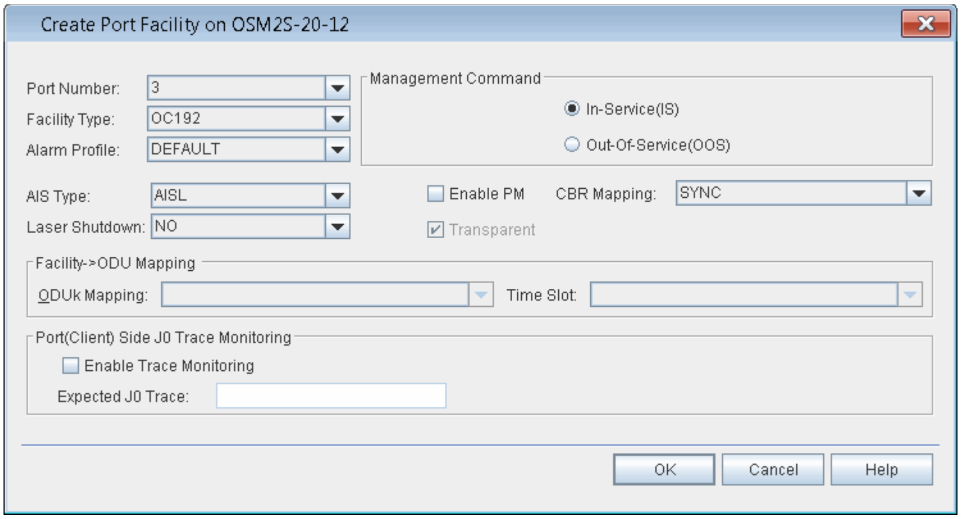
Creating OC192/STM64

10.33 This section provides an example of how to create an OC192/STM64 facility on an OSM-2S.

10.34 Create an OC192/STM64 facility by performing the following steps:

__ 1. In the **Navigation Window**, right-click the transponder icon, then click **Create Port Facility**. The **Create Port Facility** dialog box displays. Refer to Figure 10.12, page 15-213.

Figure 10.12 Create Port Facility - OSM-2S Example



Create Port Facility on OSM2S-20-12

Port Number: 3

Facility Type: OC192

Alarm Profile: DEFAULT

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

AIS Type: AISL

Laser Shutdown: NO

□ Enable PM

CBR Mapping: SYNC

☑ Transparent

Facility->ODU Mapping

ODUk Mapping:

Time Slot:

Port(Client) Side J0 Trace Monitoring

□ Enable Trace Monitoring

Expected J0 Trace:

__ 2. Click the **Port Number** drop-down box to select the port number (**1**–**20**). This is the port number on the OSM-2S that the facility interfaces.

__ 3. Click the **Facility Type** drop-down box to select the facility type. This example uses an OC-192 facility. The remaining parameters in this dialog box will be active or grayed-out depending on the facility selected.

Note: *Refer to TL1 Command Reference Manual for additional details on facility parameters. Click the Help menu in the Craft Station to access this document.*

__ 4. Click the **Alarm Profile** drop-down box to select an alarm profile (**DEFAULT**, **0**–**20**, **99**). (The default alarm profile is the default alarm profile specified at the NE level.)

__ 5. Click the **AIS Type** drop-down box and select **AISL** or **GENAIS**.

__ 6. Click the **Enable PM** check box to activate performance monitoring for the facility.

__ 7. Click the **CBR Mapping** drop-down box to select **SYNC** or **ASYNC**.

__ 8. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)**.

__ 9. Click **Laser Shutdown** drop-down box to select **YES** or **NO**.

__ 10. (optional) In the **Port(Client) Side J0 Trace Monitoring** area, click **Enable Trace Monitoring**.

__ 11. (optional) In the **Expected J0 Trace** box, type the expected J0 trace.

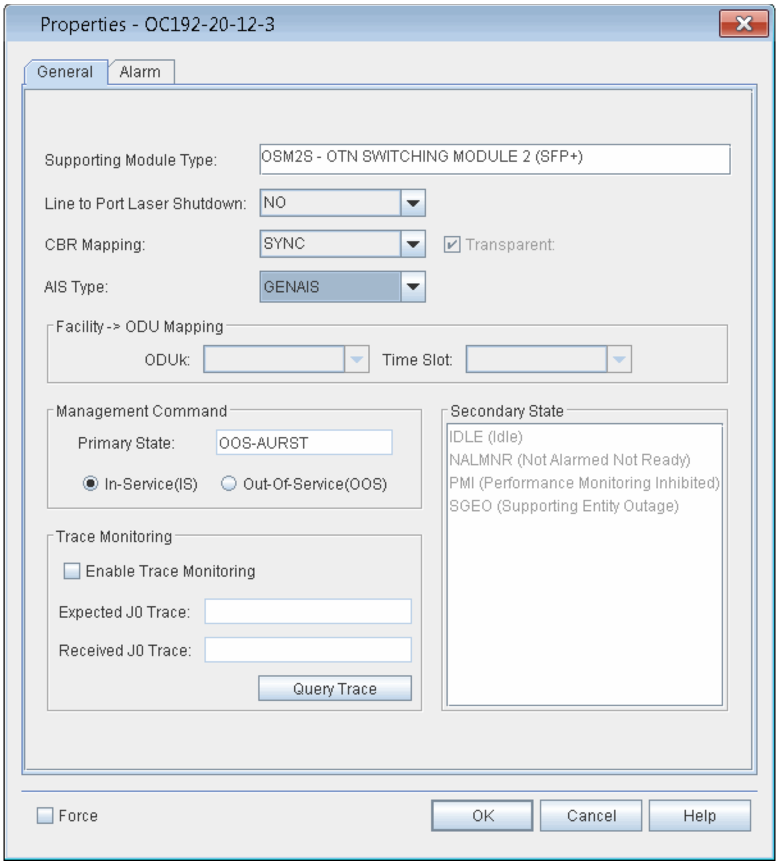
__ 12. Click **OK**.

Modifying OCn/STMn Properties

10.35 Modify the properties of an OC192/STM64 facility by performing the following steps:

__ 1. In the **Navigation Window**, expand the module icon. Right-click the **OC192** to view the shortcut menu, then click **Properties**. The **OC192 Properties** dialog box displays. Refer to Figure 10.13, page 15-214 for an example of an OC-192 supported by an SSM.

Figure 10.13 Properties - OC192



Properties - OC192-20-12-3

Supporting Module Type: OSM2S - OTN SWITCHING MODULE 2 (SFP+)

Line to Port Laser Shutdown: NO

CBR Mapping: SYNC ☑ Transparent:

AIS Type: GENAIS

Facility -> ODU Mapping

ODUk: Time Slot:

Management Command

Primary State: OOS-AURST

● In-Service(IS) ○ Out-Of-Service(OOS)

Secondary State

IDLE (Idle)
NALMNR (Not Alarmed Not Ready)
PMI (Performance Monitoring Inhibited)
SGEO (Supporting Entity Outage)

Trace Monitoring

□ Enable Trace Monitoring

Expected J0 Trace:

Received J0 Trace:

□ Force

__ 2. Click the **Line to Port Laser Shutdown** drop-down box to select **YES** or **NO**.

__ 3. Click the **CBR Mapping** drop-down box to select **SYNC** or **ASYNC**.

__ 4. Click the **AIS Type** drop-down box and select **AISL** or **GENAIS**.

__ 5. (Optional) In the **Trace Monitoring** area, configure trace monitoring by performing the following steps:

__ 5.1 Click the **Enable Trace Monitoring** box to enable trace monitoring.

__ 5.2 Click the **Insert AIS on Trace Mismatch** box to insert an alarm indication signal on trace mismatch.

__ 5.3 In the **Expected J0 Trace** box, type the expected J0 trace.

__ 6. In the **Management Command** area, the current state of the facility displays in the **Primary State** box. Click **In-Service(IS)** or **Out-Of-Service(OOS)** to change the state of the facility.

__ 7. Click the **Alarm** tab.

__ 8. Click the **Alarm Profile** drop-down box to select an alarm profile (**0**–**20**, **99**).

__ 9. Click **OK**.

Managing Facility States

10.36 This section describes managing the provisioned state of facilities. The present state of a facility may be set to in-service or out-of-service, indicating that traffic can or cannot pass.

Provisioning a Facility In-Service

10.37 Place a facility in-service by performing the following steps:

__ 1. In the **Navigation Window**, right-click the facility icon to view the shortcut menu, point to **Facility**, then click **Edit In-Service (IS from OOS_MA)**. A **Confirmation** dialog box displays asking if you are sure you want to place the facility in-service.

__ 2. Click **OK**. An Information box displays confirming that the facility is in-service.

__ 3. Click **OK**.

Provisioning a Facility Out-of-Service

10.38 Place a facility out-of-service by performing the following steps:

__ 1. In the **Navigation Window**, right-click the facility icon to view the shortcut menu, point to **Facilities**, then click **Edit Out-Of-Service (OOS_MA)**. A **Confirmation** dialog box displays.

__ 2. In the **Command Mode** area, click **Forced** or **Normal**.

Note: *Click **Forced** if you want to ignore impact on traffic and suppress alarms, events and other system messages that describe the consequences of the action. Click **Normal** if you want to view alarms, events, and other system messages that describe the consequences of the action.*

__ 3. Click **OK**. An Information box displays confirming that the facility is out-of-service.

__ 4. Click **OK**.

Deleting Facilities

10.39 Before deleting a facility, perform the following steps:

__ 1. Delete all associated port facilities and cross-connects.

__ 2. Set the facility to OOS.

__ 3. If applicable, deselect external connectivity.

__ 4. Disable performance monitoring (PM).

10.40 Delete a facility by performing the following steps:

__ 1. Right-click the facility to view the shortcut menu, then click **Delete**.

__ 2. Click **OK** in the **Confirmation** box.

Facility States

10.41 Facilities may display the following present states:

- **NR**: normal
- **ANR**: abnormal
- **RST**: restricted
- **ANRST**: abnormal and restricted
- **AU**: autonomous
- **MA**: management
- **AUMA**: autonomous and management
- **AURST**: autonomous and restricted
- **MAANR**: management and abnormal

Possible values for facility secondary state:

- **ACTIVE**: active
- **ACTTMG**: active synchronization reference
- **BERT-PRBS-TX**: transmit PRBS BER test
- **BERT-PRBS-RX**: receive PRBS BER test
- **BUSY**: busy
- **FAF**: facility failure
- **IDLE**: idle
- **LPBKF**: loopback facility
- **LPBKT**: loopback terminal
- **MT**: maintenance
- **NALMQI**: not alarmed qualified inhibit
- **PMI**: performance monitoring inhibited
- **SGEO**: supporting entity outage
- **STBY**: standby
- **STBYTMG**: standby synchronization reference

10.42 Facility protection groups may display the following states:

Possible values for present state:

- **IS**: In-Service

Possible values for present state qualifiers:

- **NR**: normal

Possible values for secondary state:

- **DNR**: do not revert
- **FSTOPROT**: force switch to protection
- **FSTOWKG**: force switch to working
- **LOCKOUT**: lockout of protection
- **MANTOPROT**: manual switch to protection
- **MANTOWKG**: manual switch to working
- **NOREQ**: no request
- **SDONWKG**: signal degrade on working
- **SDONPROT**: signal degrade on protection
- **SFONWKG**: signal fail on working
- **SFONPROT**: signal fail on protection
- **WTR**: wait-to-restore

Provisioning Y-Cable Protection

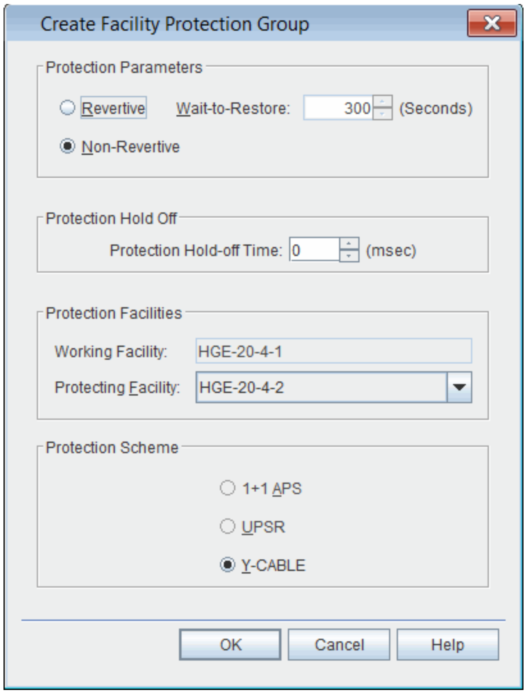
10.43 Using Y-Cable, you can provision a unidirectional protection group on port-side facilities of OSM-2Cs and OSM-2Ss.

Note: *Refer to TL1 Command Reference Manual for additional details on protection. Click the Help menu in the Craft Station to access this document.*

10.44 Create a unidirectional FFP using the Y-Cable protection scheme by performing the following steps:

__ 1. In the **Navigation Window**, right-click the port-side facility of the module to view the shortcut menu, point to **Protection Group**, then click **Create**. The **Create Facility Protection Group** dialog box displays. Refer to Figure 10.14, page 15-218.

Figure 10.14 Create Facility Protection Group (Y-Cable)


Create Facility Protection Group

Protection Parameters

○ Revertive Wait-to-Restore: 300 (Seconds)

● Non-Revertive

Protection Hold Off

Protection Hold-off Time: 0 (msec)

Protection Facilities

Working Facility: HGE-20-4-1

Protecting Facility: HGE-20-4-2

Protection Scheme

○ 1+1 APS

○ UPSR

● Y-CABLE

__ 2. In the **Protection Parameters** area, select one of the following options:

- __ **Revertive**: When the fault on the original working facility clears, that facility restores as working. In the **Wait to Restore** box, define a time interval the system should wait before it restores the affected facility to working status. The time interval can range from 0 to 3600 seconds.
- __ **Non-Revertive**: When the fault on the original working facility clears, that facility becomes the protecting facility.

__ 3. Click the **Protection Hold Off** Time up- or down-arrows to set the hold-off time between 60 msec and 1000 msec (in 5 ms increments). The Protection Hold Off value represents the amount of time before a protection switch takes place.

Note: *You can use the protection hold-off time parameter in cases where there are multiple protection domains. Setting the protection hold-off time allows other protection mechanisms to restore first before this protection group will switch.*

__ 4. Click the **Protecting Facility** drop-down box and select a facility.

__ 5. Verify that the **Protection Scheme** defaults to **Y-CABLE**.

__ 6. Click **OK**.

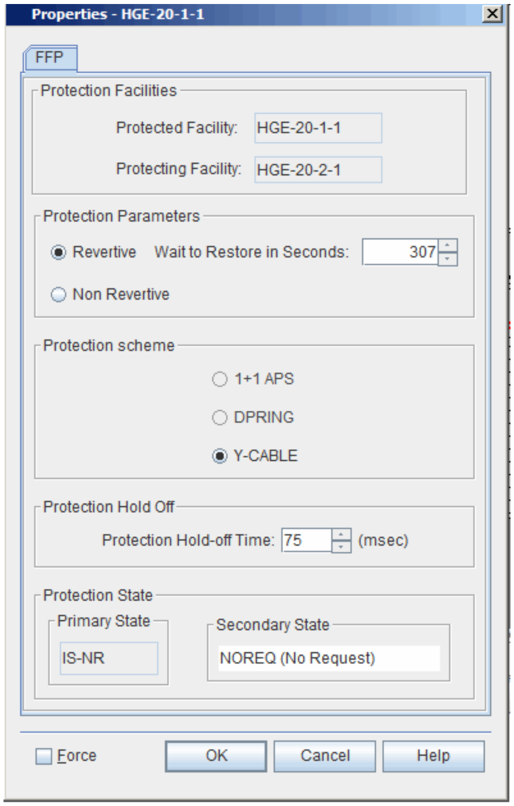
__ 7. An **Information** box displays indicating the protection group was created. Click **OK** to clear the box and the icon next to the group displays as an umbrella. A green umbrella means that the you can use the facility to carry traffic, and a blue umbrella means you cannot use the facility to carry traffic.

Viewing Y-Cable Protection Group Properties

10.45 View the properties of a Y-Cable protection group by performing the following steps:

__ 1. In the **Navigation Window**, right-click the facility protection group to view the shortcut menu, point to **Protection Properties**. The **Properties** dialog box displays. Refer to Figure 10.15, page 15-220 for an example of a Y-Cable protection group.

Figure 10.15 Y-Cable Protection Group Properties



Protection Facilities

Protected Facility: HGE-20-1-1

Protecting Facility: HGE-20-2-1

Protection Parameters

● Revertive Wait to Restore in Seconds: 307

○ Non Revertive

Protection scheme

○ 1+1 APS

○ DPRING

● Y-CABLE

Protection Hold Off

Protection Hold-off Time: 75 (msec)

Protection State

Primary State: IS-NR

Secondary State: NOREQ (No Request)

□ Force

__ 2. Review the following information:

- The **Protection Facilities** area displays Protected Facility and the Protecting Facility.
- The **Protection scheme** area defaults to Y-CABLE.
- The **Protection State** box shows the Primary State and Secondary State of the protection group.
- protection facility.

__ 3. If necessary, modify the **Protection Parameters**:

- **Revertive**: When the fault on the original working facility clears, that facility restores as working. In the **Wait to Restore in Seconds** box, define a time interval to wait before the system restores the affected facility to working status. The time interval supports a range from 0 to 3600 seconds. You can provision this setting when the protection scheme is set to 1P1 APS.
- **Non-Revertive**: When the fault on the original working facility clears, that facility becomes the protecting facility.

__ 4. If necessary, modify the **Protection Hold-Off Time**. Click the **Protection Hold Off** Time up- or down-arrows to set the hold-off time between 60 msec and 1000 msec (in 5 ms increments). The Protection Hold Off value represents the amount of time before a protection switch takes place.

Note: *You can use the protection hold-off time parameter in cases where there are multiple protection domains. Setting the protection hold-off time allows other protection mechanisms to restore first before this protection group will switch.*

__ 5. Click **OK**.

Managing Path Protection Groups

10.46 The creation of a two-way protected cross-connect between ODUk facilities supported by an OSM-2C or OSM-2S implicitly creates a path protection (ODU SNC protection) group. When you cross connect the port facilities that are mapped to the ODUk facilities across the switch fabric, the facilities are protected using Subnetwork Connection Protection-Inherent (SNC-I) or Subnetwork Connection Protection-Non-Intrusive (SNC-N).

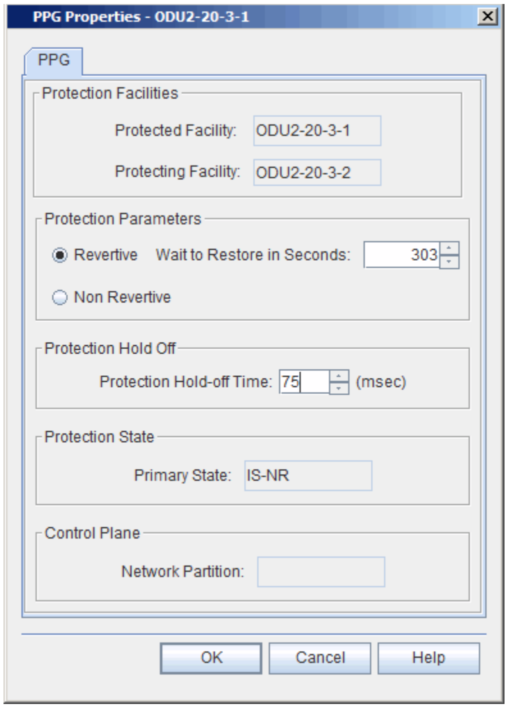
10.47 For information about creating an ODUk cross-connect on an OSM-2C or OSM-2S, refer to Creating ODUk Cross-Connects on OTN Switching Module, page 15-226.

10.48 Manage a path protection group by performing the following steps:

__ 1. In the **Navigation Window**, expand the ODUk facilities supported by the OSM-2C or OSM-2S.

__ 2. Right-click the selected ODUk supporting the cross-connect to view the shortcut menu, then click **PPG Properties**. The **PPG Properties** dialog box displays. Refer to Figure 10.16, page 15-221.

Figure 10.16 PPG Properties



PPG Properties - ODU2-20-3-1

PPG

Protection Facilities

Protected Facility: ODU2-20-3-1

Protecting Facility: ODU2-20-3-2

Protection Parameters

● Revertive Wait to Restore in Seconds: 303

○ Non Revertive

Protection Hold Off

Protection Hold-off Time: 75 (msec)

Protection State

Primary State: IS-NR

Control Plane

Network Partition:

__ 3. If necessary, modify the **Protection Parameters**:

- **Revertive**: When the fault on the original working facility clears, that facility restores as working. In the **Wait to Restore in Seconds** box, define a time interval to wait before the system restores the affected facility to working status. The time interval supports a range from 0 to 3600 seconds.
- **Non-Revertive**: When the fault on the original working facility clears, that facility becomes the protecting facility.

__ 4. If necessary, modify the **Protection Hold-Off Time**. Click the **Protection Hold Off** Time up- or down-arrows to set the hold-off time between 60 msec and 1000 msec (in 5 ms increments). The Protection Hold Off value represents the amount of time before a protection switch takes place.

Note: *You can use the protection hold-off time parameter in cases where there are multiple protection domains. Setting the protection hold-off time allows other protection mechanisms to restore first before this protection group will switch.*

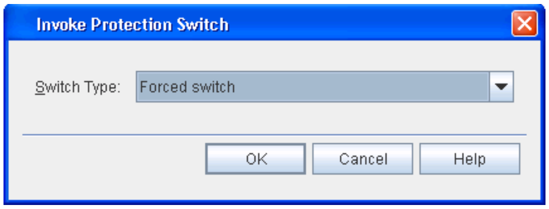
__ 5. Click **OK**.

Managing Path Protection Group Switches

10.49 You can configure a real-time protection switch on a path protection (ODU SNC protection) group. Manage a protection switch by performing the following steps:

__ 1. In the **Navigation Window**, right-click the ODUk facility supporting the cross-connect, point to **Protection Switch**, then click **Invoke**. The **Invoke Protection Switch** dialog box displays. Refer to Figure 10.17, page 15-222.

Figure 10.17 Invoke Protection Switch



Switch Type: Forced switch

__ 2. Click the **Switch Type** drop-down box to select one of the following:

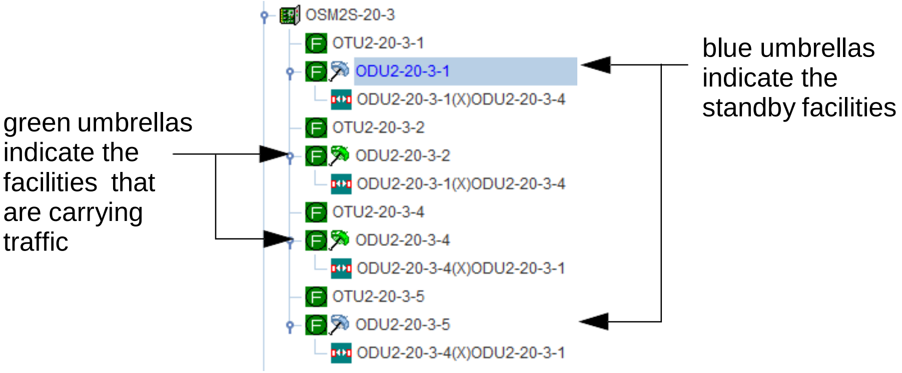
- **Forced switch** (A forced switch forces an immediate switch to defined protecting facility. No warning messages display during the switch. Selecting a forced switch may affect traffic.)
- **Manual switch** (During a manual switch the system displays warning messages during the switch, including messages that indicate if traffic may drop during the switch.)
- **Lockout of protection switching** (Lockout of protection switching prevents protection switching.)

__ 3. Click **OK**.

10.50 Release a protection switch on the selected protection switch group by clicking **Release** from the shortcut menu.

10.51 In the Navigation Window, the icons next to the protection switch indicate the status of the switch. Refer to Figure 10.18, page 15-223.

Figure 10.18 Protection Switch Icon Before Switch


OSM2S-20-3
OTU2-20-3-1
ODU2-20-3-1
ODU2-20-3-1(X)ODU2-20-3-4
OTU2-20-3-2
ODU2-20-3-2
ODU2-20-3-1(X)ODU2-20-3-4
OTU2-20-3-4
ODU2-20-3-4
ODU2-20-3-4(X)ODU2-20-3-1
OTU2-20-3-5
ODU2-20-3-5
ODU2-20-3-4(X)ODU2-20-3-1

green umbrellas indicate the facilities that are carrying traffic

blue umbrellas indicate the standby facilities

Deleting a Path Protection Group

10.52 In order to delete a PPG, modify the cross-connect to be unprotected by removing one of its legs. Delete a path protection (ODU SNC protection) group by performing the following steps:

__ 1. In the **Navigation Window**, right-click one of the facilities supporting the cross-connect to view the shortcut menu, point to **Facility**, then click **Edit Out-Of-Service (OOS-MA)**. A **Confirmation** box displays asking if you want to place the facility in the out-of-service state.

__ 2. Click **Forced**.

Note: *Click **Forced** if you want to ignore impact on traffic and suppress alarms, events and other system messages that describe the consequences of the action. Click **Normal** if you want to view alarms, events, and other system messages that describe the consequences of the action.*

__ 3. Click **OK**.

__ 4. In the **Navigation Window**, right-click the cross-connect to view the shortcut menu, then click **Properties**. The **Properties** dialog box displays.

__ 5. Change either the source protection or destination protection box to be blank.

__ 6. Click **OK**. The PPG and protecting leg are removed.

Deleting a Y-Cable Protection Group

10.53 Complete the following steps to remove Y-Cable protection:

__ 1. In the **Navigation Window**, expand the impacted module.

__ 2. Before you can delete the protection group, you must place one of the facilities out-of-service (OOS). Choose either the working or protecting facility. Optionally, you can place both facilities OOS.

__ 3. Right-click the impacted facility, point to Facility, then click **Edit Out-Of-Service(OOS-MA)** to shut down the port laser. A lock icon displays next to the facility in the **Navigation Window**.

Note: *The laser of an OOS facility will always stay off while it is part of the protection group (FFP). However, once the protection group has been deleted the laser will only stay off temporarily. Any state change of the facility will cause the supporting laser to turn back on.*

__ 4. (Optional) In order to ensure that the laser of the OOS facility remains off regardless of any state changes, place the supporting port equipment OOS. Right-click the pluggable transceiver or optical equipment supporting the impacted facility, point to **Module**, then click **Edit Out-Of-Service(OOS-MA)**.

__ 5. Right-click the impacted facility, point to **Protection Group**, then click **Delete**.

> ***Warning:***
>
> *Some equipment optics may be temporarily or permanently damaged if both lasers transmitting on a Y-cable turn on simultaneously. Remove the fiber connections to avoid this scenario.*

__ 6. Remove the physical Y-cable fiber connections. This step must be performed immediately after you delete the protection group.

__ 7. (Optional) If you placed the pluggable transceiver supporting the impacted facility OOS in step 4, page 15-224, place the equipment IS after the Y-cable fibers have been removed. Right-click the pluggable transceiver supporting the impacted facility, point to **Module**, then click **Edit In-Service(IS from OOS-MA)**.

11. Provisioning Cross-Connects

11.1 This section provides procedures for creating cross-connects in the mTera.

Note: *For detailed descriptions of system cross-connects, refer to TL1 Command Reference Manual. Click the Help menu in the Craft Station to access this document.*

Cross-Connect Properties

11.2 The following fields display in cross-connect-related dialog boxes:

- Software formats cross-connect addresses as follows:

  ODU2-20-5-2-1 X ODU2-20-2-2 represents an ODU2 cross-connect between an ODU2 supported by an OSM-2C in shelf 20, slot 5, port 2, timeslot 1. The facility is cross-connected to an ODU2 supported by an OSM-2S in shelf 20, slot 2, port 2.
- **From Channel**: Optical channel that is source of cross-connect
- **To Channel**: Optical channel that is destination of cross-connect
- **Type**: Cross-connect type:
  - **2WAY**: Path is bi-directional.
  - **2WAYPR**: Path is bi-directional for SNCP protection.
  - **2WAYDRI**: Path is bi-directional for dual ring interconnection.
  - **1WAY**: Path is one direction only.
  - **1WAYPR**: Path is one direction only for SNCP protection.
- **Source Protection ID**: Facility protecting the "From Channel" ODUk
- **Destination Protection ID**: Facility protecting the "To Channel" ODUk
- **Circuit ID**: The circuit being provisioned.
- **Source Protection Type**: **Non-intrusive** or **Inherent** (SNC/I or SNC/N)
- **Destination Protection Type**: **Non-intrusive** or **Inherent** (SNC/I or SNC/N)
- **Source Protection Type Status**
- **Destination Protection Type Status**
- **Other NE Info**: When cross-connect is between NEs, this field identifies the destination NE.
- **Group ID**: Group Broadcast or Drop/Continue cross-connects using common OCH facilities within the same NE by defining a 31-digit, alphanumeric Group ID.

- **PST**: Indicates the present state of the entity:
  - **IS**: In-Service
  - **OOS**: Out-Of-Service

  A further qualifier may display as described below:
  - **NR**: normal
  - **ANR**: abnormal
  - **AU**: autonomous
- **SST**: Indicates the secondary state of the entity:
  - **SGEO**: supporting entity outage
  - **RDLD**: red-lined
- **RedLined**: Specifies if the facility is red-lined (a red-lined cross-connect cannot be deleted without a forced prompt).
- **Included**: If you check this box, you can delete the cross-connect without a forced prompt.
- **NP Owner**: control plane network partition owner of this entity.

Creating Facility Cross-Connects

11.3 This section gives examples of specific cross-connect types and the associated provisionable fields:

- Creating ODUk Cross-Connects on OTN Switching Module, page 15-226

Creating ODUk Cross-Connects on OTN Switching Module

11.4 OTN switching modules support mapping supported client facilities to an ODUk facility. You can cross-connect ODUk facilities across the switch fabric to support ODUk switching.

Note: *For more information about ODUk cross-connects, refer to the ENT-CRS-ODUk command in the TL1 Command Reference Manual. Click the Help menu in the Craft Station to access this document.*

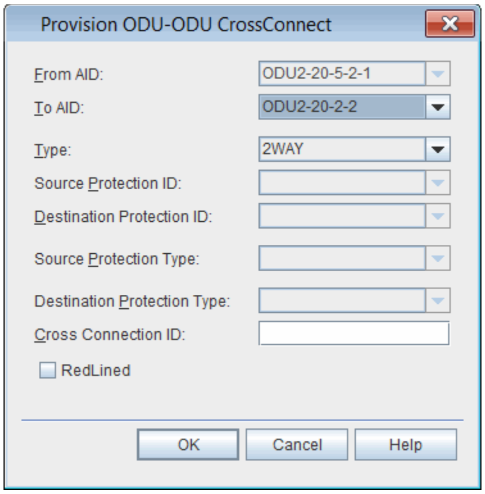
11.5 Create an ODUk cross-connect by performing the following steps:

__ 1. If necessary, provision ODUk facilities on the module. Refer to Optical Data Unit (ODU) Facilities, page 15-196.

__ 2. If necessary, create client facilities and map the client facilities to the ODUk facilities. Refer to ODU Multiplexing, page 15-199 for more information.

__ 3. In the Navigation Window, right-click the ODUk facility to view the cross-connect, then click **Create CrossConnect**. The **Provision ODU-ODU CrossConnect** dialog box displays. Refer to Figure 11.1, page 15-227.

Figure 11.1 Provision ODU-ODU CrossConnect



Provision ODU-ODU CrossConnect

From AID: ODU2-20-5-2-1

To AID: ODU2-20-2-2

Type: 2WAY

Source Protection ID:

Destination Protection ID:

Source Protection Type:

Destination Protection Type:

Cross Connection ID:

□ RedLined

__ 4. Verify that the location of the facility you are provisioning displays in the **From AID** box.

__ 5. Click the **To AID** drop-down box to select the facility for the far-end of the cross-connect.

__ 6. Click the **Type** drop-down box to select the cross-connection type (**2WAY**, **2WAYPRI**, **2WAYDRI**, **1WAY**, **1WAYPR**) The default is 2WAY.

__ 7. If you are creating a 2WAYPR type cross-connection, complete the following steps. Otherwise, go to step 8, page 15-227.

Note: *The creation of the 2WAYPR cross-connect implicitly creates the PPG (Path Protection Group).*

__ 7.1 Click the **Source Protection ID** drop-down box to select the AID of the facility providing the source of the protected cross-connect.

__ 7.2 Click the **Destination Protection ID** drop-down box to select the AID of the facility providing the destination of the protected cross-connect.

__ 7.3 Click the **Source Protection Type** drop-down box to select **Non-intrusive** or **Inherent**.

__ 7.4 Click the **Destination Protection** type drop-down box to select **Non-intrusive** or **Inherent**.

__ 8. (optional) In the **Connection ID** box, type a name for the cross-connect.

__ 9. Click the **RedLined** box to red line the cross-connect. (If a cross-connect is RedLined, delete it by selecting Forced in the Delete Cross-Connection dialog box.)

__ 10. Click **OK**.

Modifying an ODUk Cross-Connection Protected and Unprotected Status

11.6 This section describes how to change the protected or unprotected status of an ODUk cross-connection.

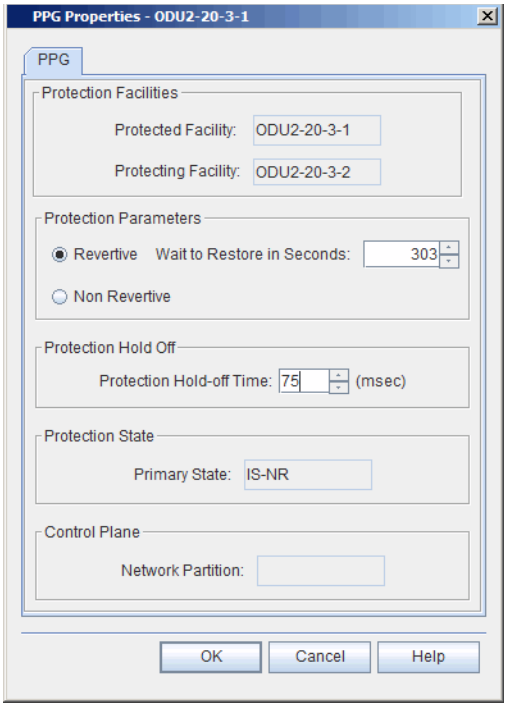
Modifying ODUk Cross-Connection from Protected to Unprotected

11.7 Edit an ODUk cross-connection from protected to unprotected status by performing the following steps:

__ 1. Verify that the ODU PPG is non-revertive by performing the following steps:

__ 1.1 In the **Navigation Window**, right-click the ODUk supporting the cross-connect to view the shortcut menu, then click **PPG Properties**. The **PPG Properties** dialog box displays. Refer to Figure 11.2, page 15-228.

Figure 11.2 PPG Properties



PPG Properties - ODU2-20-3-1

PPG

Protection Facilities

Protected Facility: ODU2-20-3-1

Protecting Facility: ODU2-20-3-2

Protection Parameters

● Revertive Wait to Restore in Seconds: 303

○ Non Revertive

Protection Hold Off

Protection Hold-off Time: 75 (msec)

Protection State

Primary State: IS-NR

Control Plane

Network Partition:

__ 1.2 Choose one of the following options:

If the PPG is Revertive, go tostep 1.3, page 15-229.

If the PPG is Non Revertive, go to step 2, page 15-229.

__ 1.3 Click **Non Revertive** to change the protection type of the PPG.

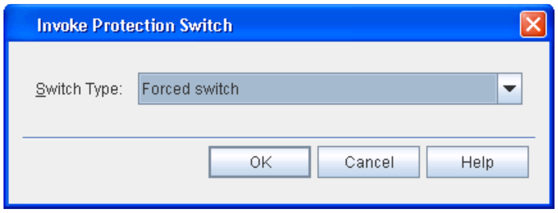
__ 1.4 Click **OK**.

__ 2. Force a protection switch in the PPG by performing the following steps:

__ 2.1 Identify the active ODUk in the PPG.

__ 2.2 Right click the active ODUk facility to view the shortcut menu, point to **Protection Switch**, then click **Invoke**. The **Invoke Protection Switch Dialog** box displays. Refer to Figure 11.3, page 15-229.

Figure 11.3 Invoke Protection Switch



Invoke Protection Switch

Switch Type: Forced switch

__ 2.3 Click the **Switch Type** drop-down box to select **Forced switch**.

__ 2.4 Click **OK**.

__ 2.5 In the **Navigation Window**, the icons next to the ODUk facilities indicate the status of the switch. Verify the status of the switch. Refer to paragraph 9.103, page 15-277.

__ 3. Release the protection switch by performing the following steps:

__ 3.1 Right click the active ODUk facility to view the shortcut menu, point to **Protection Switch**, then click **Release**. A **Confirmation** box displays asking if you want to release the protection switch.

__ 3.2 Click **OK**.

__ 4. Edit the ODUk facility to be removed from the cross-connection in the out-of-service state by performing the following steps:

__ 4.1 In the **Navigation Window**, right-click the ODUk facility to view the shortcut menu, then click **Properties**. The **Properties** dialog box displays.

__ 4.2 Click the **State Tab**.

__ 4.3 In the **Management Command** area, click **Out-Of-Service (OOS)**.

__ 4.4 In the **Command Mode** area, click **Forced** or **Normal**.

__ 4.5 Click **OK**.

__ 5. Remove the ODUk leg from the cross-connection to convert from a protected to unprotected cross-connection by removing the ODUk leg. Perform the following steps:

__ 5.1 In the **Navigation Window**, right-click the cross-connection to view the shortcut menu, then click **Properties**. The **Properties** dialog box displays.

__ 5.2 Click either the **Source Protection ID** or **Destination Protection ID** drop-down box to remove the ODUk leg from the cross-connection. Select the blank entry in order to remove the leg.

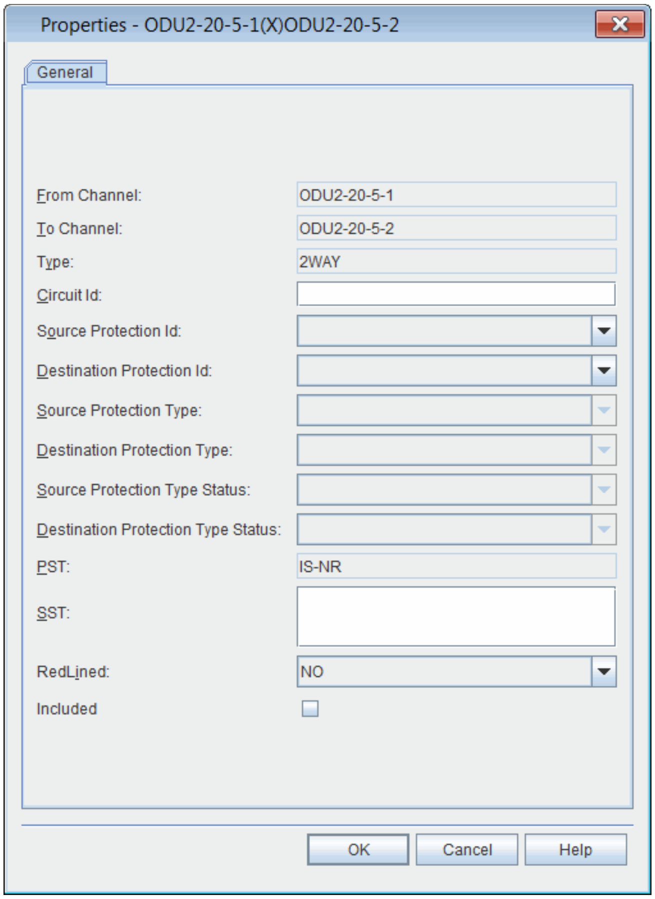
__ 5.3 Click **OK**.

Modifying ODUk Cross-Connection from Unprotected to Protected

11.8 Edit an ODUk cross-connection from unprotected to protected status by performing the following steps:

__ 1. In the **Navigation Window**, right-click the cross-connect to view the shortcut menu, then click **Properties**. The **Properties** dialog box displays. Refer to Figure 11.4, page 15-231 for an example of the **Properties** dialog box for an unprotected two-way ODU2-to-ODU2 cross-connect.

Figure 11.4 2WAY Unprotected Cross-Connect Properties



Properties - ODU2-20-5-1(X)ODU2-20-5-2

General

From Channel: ODU2-20-5-1

To Channel: ODU2-20-5-2

Type: 2WAY

Circuit Id:

Source Protection Id:

Destination Protection Id:

Source Protection Type:

Destination Protection Type:

Source Protection Type Status:

Destination Protection Type Status:

PST: IS-NR

SST:

RedLined: NO

Included ☐

__ 2. Click the **Source Protection ID** drop-down box to select the protecting facility.

__ 3. Click the **Destination Protection ID** drop-down box to select the protecting facility.

__ 4. Click **OK**. The creation of a 2WAYPR cross-connect automatically creates the PPG, and the cross-connect is now protected.

Deleting Cross-Connects

11.9 Delete a cross-connect by performing the following step:

__ 1. In the **Navigation Window**, expand the associated facility to display the cross-connect. Right-click the cross-connect to display the shortcut menu, then click **Delete**. An **Information** box displays. Click **OK**.

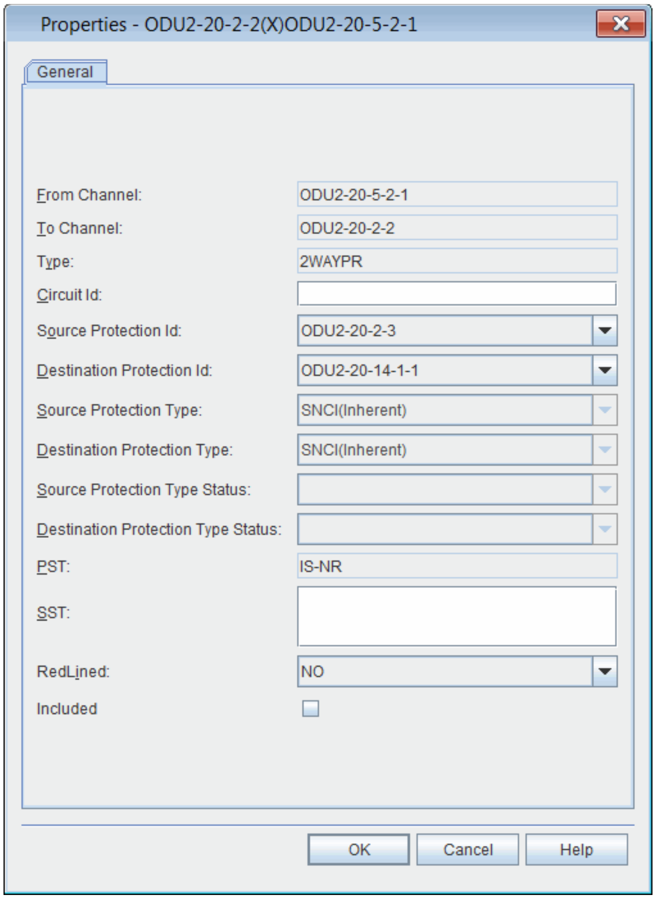
Viewing Cross-Connect Properties

11.10 View the properties of a provisioned cross-connect by performing the following steps:

__ 1. In the **Navigation Window**, expand the associated module and facility to display the cross-connect.

__ 2. Right-click the cross-connect to view the shortcut menu, then click **Properties**. Refer to Figure 11.5, page 15-232 for an example of the **Properties** dialog box for an ODU2-to-ODU2 cross-connect.

Figure 11.5 Cross-Connect Properties



From Channel: ODU2-20-5-2-1

To Channel: ODU2-20-2-2

Type: 2WAYPR

Circuit Id:

Source Protection Id: ODU2-20-2-3

Destination Protection Id: ODU2-20-14-1-1

Source Protection Type: SNCI(Inherent)

Destination Protection Type: SNCI(Inherent)

Source Protection Type Status:

Destination Protection Type Status:

PST: IS-NR

SST:

RedLined: NO

Included ☐

Wavelength/Channel/Frequency Associations

11.11 Table 11.1, page 15-233 and Table 11.1, page 15-233 identify the wavelength associations between channels and frequencies in the NE. Refer to Provisioning Cross-Connects, page 15-225 for detailed information on provisioning wavelengths.

88-Channel Systems

11.12 Refer to Table 11.1, page 15-233 for the 88-channel wavelength plan.

Table 11.1 88-Channel Wavelength/Frequency Plan

Wavelength (nm)	Channel ID	Frequency (THz)	Wavelength (nm)	Channel ID	Frequenc y (THz)
1563.86	1	191.7	1563.45	45	191.75
1563.05	2	191.8	1562.64	46	191.85
1562.23	3	191.9	1561.83	47	191.95
1561.42	4	192.0	1561.01	48	192.05
1560.61	5	192.1	1560.20	49	192.15
1559.79	6	192.2	1559.39	50	192.25
1558.98	7	192.3	1558.58	51	192.35
1558.17	8	192.4	1557.77	52	192.45
1557.36	9	192.5	1556.96	53	192.55
1556.55	10	192.6	1556.15	54	192.65
1555.75	11	192.7	1555.34	55	192.75
1554.94	12	192.8	1554.54	56	192.85
1554.13	13	192.9	1553.73	57	192.95
1553.33	14	193.0	1552.93	58	193.05
1552.52	15	193.1	1552.12	59	193.15
1551.72	16	193.2	1551.32	60	193.25
1550.92	17	193.3	1550.52	61	193.35
1550.12	18	193.4	1549.72	62	193.45
1549.32	19	193.5	1548.91	63	193.55
1548.51	20	193.6	1548.11	64	193.65
1547.72	21	193.7	1547.32	65	193.75
1546.92	22	193.8	1546.52	66	193.85
1546.12	23	193.9	1545.72	67	193.95
1545.32	24	194.0	1544.92	68	194.05
1544.53	25	194.1	1544.13	69	194.15
1543.73	26	194.2	1543.33	70	194.25
1542.94	27	194.3	1542.54	71	194.35
1542.14	28	194.4	1541.75	72	194.45

Table 11.1 88-Channel Wavelength/Frequency Plan (Continued)

Wavelength (nm)	Channel ID	Frequency (THz)	Wavelength (nm)	Channel ID	Frequenc y (THz)
1541.35	29	194.5	1540.95	73	194.55
1540.56	30	194.6	1540.16	74	194.65
1539.77	31	194.7	1539.37	75	194.75
1538.98	32	194.8	1538.58	76	194.85
1538.19	33	194.9	1537.79	77	194.95
1537.40	34	195.0	1537.00	78	195.05
1536.61	35	195.1	1536.22	79	195.15
1535.82	36	195.2	1535.43	80	195.25
1535.04	37	195.3	1534.64	81	195.35
1534.25	38	195.4	1533.86	82	195.45
1533.47	39	195.5	1533.07	83	195.55
1532.68	40	195.6	1532.29	84	195.65
1531.90	41	195.7	1531.51	85	195.75
1531.12	42	195.8	1530.72	86	195.85
1530.33	43	195.9	1529.94	87	195.95
1529.55	44	196.0	1529.16	88	196.05

12. Control Plane

12.1 This section describes the NP-1 is the management communications network (MCN) partition of control plane, which carries the management traffic.

- Control Plane Network Partition, page 15-235 - information about how to configure the MCN network partition
  - Provisioning Signaling Communications within the MCN, page 15-236
- Managing Nodes, page 15-247 - information about how to view or modify the properties of an MCN node
- Managing TLs, page 15-249 - information about how to view or modify the properties of topological links
- Managing Routing and Signaling Elements, page 15-252 - information about how to view and modify the properties of the routing and signaling elements of the MCN nodes

Control Plane Network Partition

12.2 A Network Partition allows you to configure the management communications network (MCN).

12.3 The MCN is used by the management system for IP connectivity using external Ethernet network or internal embedded operations network (EON). Provision the OSPF, OSPF Area, and NODE for the MCN to enable routing and signalling communications.

12.4 Use the AID of NP-1 for the MCN partition.

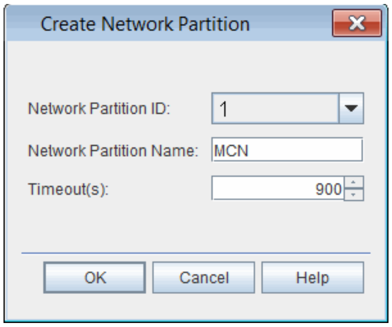
Creating MCN Partition

12.5 This section describes how to create the management communications network (MCN) partition.

12.6 Create an MCN partition by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **Control Plane** icon to view the shortcut menu, then click **Create Network Partition**. The **Create Network Partition** dialog box displays. Refer to Figure 12.1, page 15-236.

Figure 12.1 Create Network Partition



Create Network Partition

Network Partition ID: 1

Network Partition Name: MCN

Timeout(s): 900

__ 2. Click the **Network Partition ID** drop-down box to select **1**.

__ 3. (optional) In the **Network Partition Name** box, type a name for the MCN partition (**0**–**30** characters).

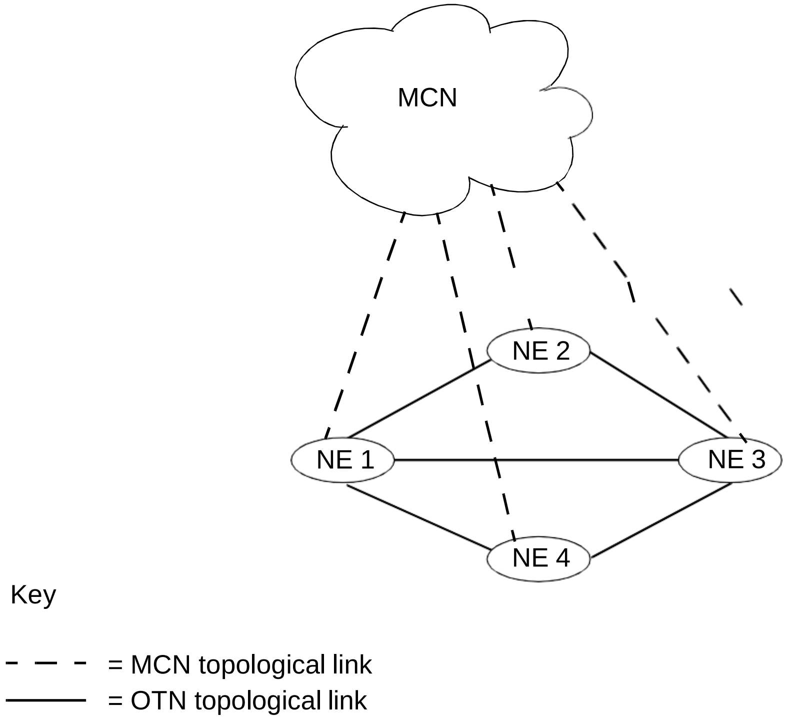
__ 4. Click the **Timeout** drop-down box to select the default timeout for a call setup request (**10** seconds–**900** seconds.) The system defaults to 120 seconds.

__ 5. Click **OK**.

Provisioning Signaling Communications within the MCN

12.7 This section describes how to create the signaling communication entities within the MCN partition. The signaling communication entities define the network that carries the control plane routing and signaling messages. Routing protocols advertise the optical network topologies and the available bandwidth resources within and between the network domains. Control plane uses signaling protocols for provisioning, maintaining, and deleting connections. Refer to Figure 12.2, page 15-237.

Figure 12.2 MCN Domain



12.8 Table 12.1, page 15-237 lists the network identifiers necessary to configure signaling communication entities within the MCN partition. Plan the network identifiers for each NE within the MCN.

Table 12.1 Network Identifiers for MCN Partition

NE Network Identifiers	Description	Example	Value
OSPF routing controller ID	unique value for each NE in MCN	110.1.2.1	
MCN node ID	unique value for each NE in MCN	130.200.2.1	
near end address of SINTF-1	unique value for each NE in MCN	130.200.2.1	
near end address of Ethernet port	unique value for each NE in MCN	130.1.2.2	
OSPF routing area	all NEs in the MCN use the same routing area	100.1.2.1	

12.9 Provision signaling communications within the MCN partition by performing the following steps:

1. Creating Routing Controller, page 15-238
2. Creating OSPF Area, page 15-238
3. Creating Node for MCN Partition, page 15-240
4. Creating TL for an Ethernet Signaling Port in the MCN, page 15-245
5. Repeat steps 1, page 15-237 through 4, page 15-237 at each NE within the MCN.

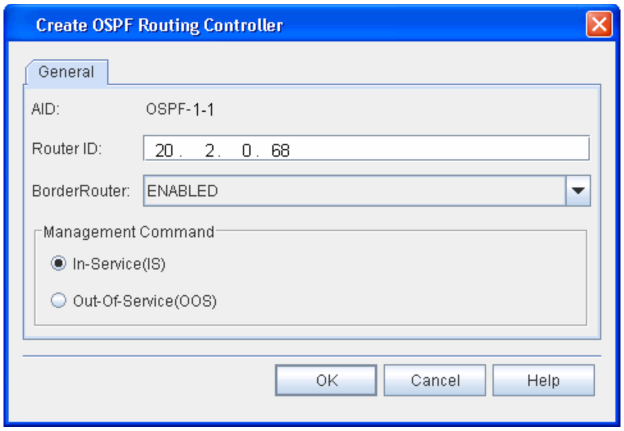
Creating Routing Controller

12.10 Create the routing controller by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-1** icon to view the shortcut menu, then click **Routing**. The **Routing** tabbed view displays.

__ 2. Verify the **OSPF Routing Controller** tab is selected. Click **Create.** The **Create OSPF Routing Controller** dialog box displays. Refer to Figure 12.3, page 15-238.

Figure 12.3 Create OSPF Routing Controller



Create OSPF Routing Controller

General

AID: OSPF-1-1

Router ID: 20 . 2 . 0 . 68

BorderRouter: ENABLED

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

__ 3. In the **Router ID** box, type the router ID address (for example, **110.1.2.1**).

__ 4. Click the **Border Router** drop-down box to specify if this OSPF router is a border router (**ENABLED** or **DISABLED**).

__ 5. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)** to set the state of the OSPF router.

__ 6. Click **OK**. The newly created OSPF router displays in the **OSPF Routing Controller** table.

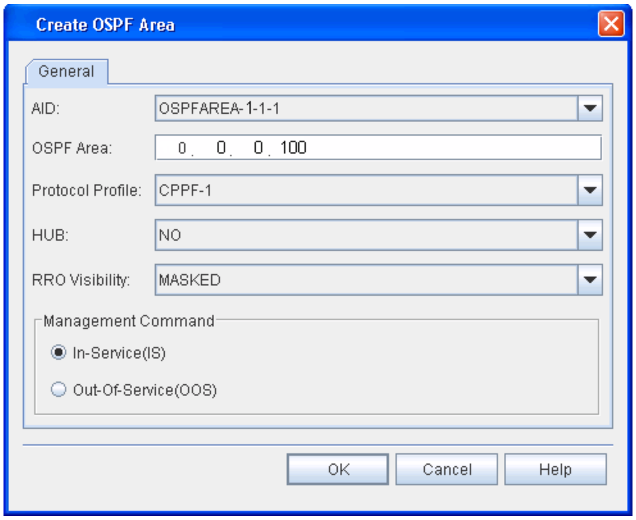
Creating OSPF Area

12.11 Create an OSPF area by performing the following steps:

__ 1. In the **Routing** tabbed view, click the **OSPF Area** tab.

__ 2. Click **Create**. The **Create OSPF Area** dialog box displays. Refer to Figure 12.4, page 15-239.

Figure 12.4 Create OSPF Area



Create OSPF Area

General

AID: OSPFAREA-1-1-1

OSPF Area: 0 . 0 . 0 . 100

Protocol Profile: CPPF-1

HUB: NO

RRO Visibility: MASKED

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

__ 3. Click the **AID** drop-down box to select the **OSPF AID**. (For example, select **OSPFAREA-1-1-1** for the first NE. The system supports up to 32 OSPF AIDs.)

__ 4. In the **OSPF Area** box, type the router ID (for example, **0.0.0.100**).

__ 5. Click the **Protocol Profile** drop-down box to select the AID of the control plane protocol profile (CPPF-1 to CPPF-20, CPPF-94 to CPPF-99).

__ 6. Click the **HUB** drop-down box to select **YES** (if the OSPF area is a hub) or **NO** (if the OSPF area is not a hub).

__ 7. Click the **RRO Visibility** drop-down box to select **PASSED** (recorded route object for this area is to be propagated outside of the area as well as within the area) or **MASKED** (recorded route object for this area is to be propagated within the area but not to be propagated outside of the area).

__ 8. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)** to set the state of the OSPF area.

__ 9. Click **OK**. The newly created OSPF routing area displays in the **OSPF Area** table.

Note: *Refer to Managing OSPF Area Properties, page 15-255 for information about modifying the properties of the OSPF area.*

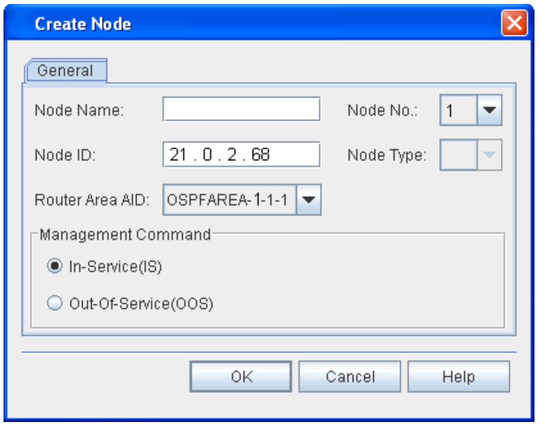
Creating Node for MCN Partition

12.12 Create the node for the MCN partition by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-1** icon to view the shortcut menu, then click **Nodes and Links**. The **Nodes and Links** tabbed view displays.

__ 2. Verify the **Node** tab is selected, then click **Create**. The **Create Node** dialog box displays. Refer to Figure 12.5, page 15-240.

Figure 12.5 Create Node



Node Name:

Node No.: 1

Node ID: 21 . 0 . 2 . 68

Node Type:

Router Area AID: OSPFAREA-1-1-1

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

__ 3. (optional) In the **Node Name** box, type a name for the MCN node (0–30 characters).

__ 4. In the **Node ID** box, type the Node ID (for example, 130.200.2.1). The Node ID must be unique within the node's area.

__ 5. Click the **Router Area Aid** drop-down box to select the OSPFAREA AID to associate with this node.

__ 6. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)** to set the state of the node.

__ 7. Click **OK**.

Create IP Protection Group

12.13 An IP Protection Group (IPPG) is a virtual entity representing a protection group for the IP address supported on two physical DCN interfaces.

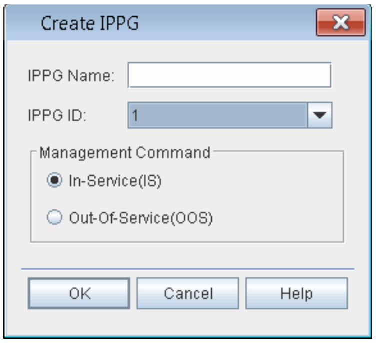
12.14 You can assign a single IP address to the IP protection group by provisioning a TL (with the IPPG entity as the resource of the TL). The IP address will be protected between the members of the IPPG.

12.15 The SEIM port can be the member of the IPPG, which is provisioned by the ENT-MGTETH command.

12.16 Create an IP protection group for the NP-1 partition by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-1** icon to view the shortcut menu, then click **Create IPPG**. The **Create IPPG** dialog box displays. Refer to Figure 12.6, page 15-241.

Figure 12.6 Create IPPG


Create IPPG

IPPG Name:

IPPG ID: 1

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

__ 2. In the **IPPG** name box, type a name for the entity (0–30 characters).

__ 3. Click the **IPPG ID** drop-down box to select the AID (**1**).

__ 4. In the **Management Command** area, click **OOS (Out of Service)** or **IS (In Service)** to set the state of the entity.

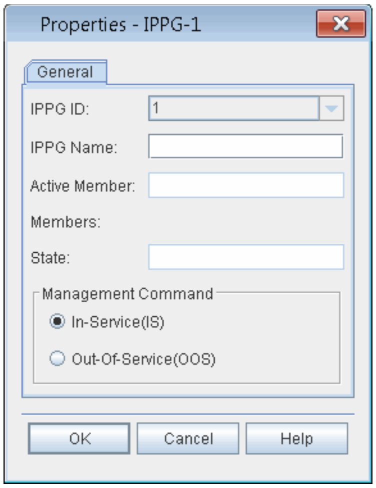
__ 5. Click **OK**.

Modifying IPPG

12.17 Modify the properties of an IPPG by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **IPPG** to view the shortcut menu, the click **Properties**. The **Properties - IPPG** dialog box displays. Refer to Figure 12.7, page 15-241.

Figure 12.7 Properties - IPPG


Properties - IPPG-1

General

IPPG ID: 1

IPPG Name:

Active Member:

Members:

State:

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

__ 2. (Optional) In the **IPPG** name box, type a name for the entity (0–30 characters).

__ 3. View the member of the IPPG in the **Active Member** box.

__ 4. In the **Management Command** area, click **OOS (Out of Service)** or **IS (In Service)** to set the state of the entity.

__ 5. Click **OK**.

Deleting IPPG

12.18 Delete an IPPG by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **IPPG** to view the shortcut menu, the click **Delete**.

__ 2. A **Confirmation** box displays asking if you want to delete the IPPG.

__ 3. Click **OK**.

Creating TL

12.19 The following steps describe the generic procedure for creating a topological link (TL).

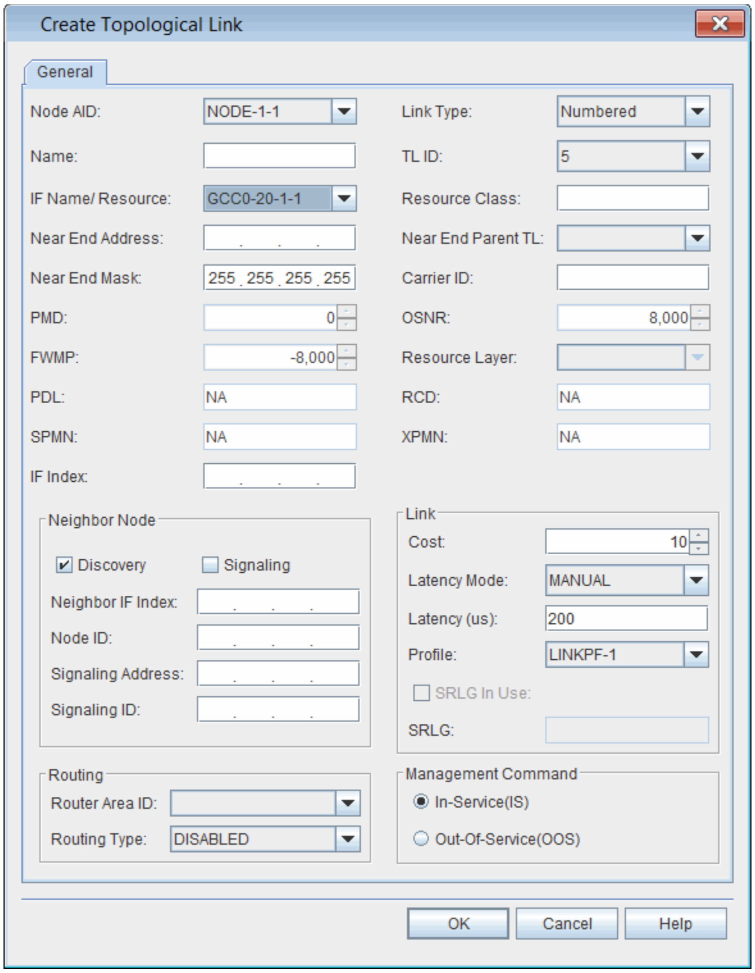
12.20 For more information about the parameters available when creating a TL, refer to the ENT-TL command in *TL1 Command Reference Manual*.

12.21 Create a TL by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-x** icon to view the shortcut menu, then click **Nodes and Links**. The **Nodes and Links** tabbed view displays.

__ 2. Click the **Topological Link** tab, then click **Create**. The **Create Topological Link** dialog box displays. Refer to Figure 12.8, page 15-243.

Figure 12.8 Create Topological Link



Create Topological Link

General

Node AID:	NODE-1-1	Link Type:	Numbered
Name:		TL ID:	5
IF Name/ Resource:	GCC0-20-1-1	Resource Class:	
Near End Address:	. . .	Near End Parent TL:	
Near End Mask:	255 . 255 . 255 . 255	Carrier ID:	
PMD:	0	OSNR:	8,000
FWMP:	-8,000	Resource Layer:	
PDL:	NA	RCD:	NA
SPMN:	NA	XPMN:	NA
IF Index:	. . .		

Neighbor Node

☑ Discovery □ Signaling

Neighbor IF Index: . . .

Node ID: . . .

Signaling Address: . . .

Signaling ID: . . .

Link

Cost: 10

Latency Mode: MANUAL

Latency (us): 200

Profile: LINKPF-1

□ SRLG In Use:

SRLG:

Routing

Router Area ID:

Routing Type: DISABLED

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

__ 3. Click the **Node AID** drop-down box to select the Node AID (for example, NODE-1-1).

__ 4. (optional) In the **Name** box, type a name for the TL (0–30 characters).

__ 5. Click the **IF Name/Resource** to select the stable interface name (for example, SINTF-1, GCC, MGTETH, IPPG).

__ 6. If necessary, type the address of the near end of the TL in the **Near End Address** box (for example, 130.200.2.1).

__ 7. If necessary, type the near end mask address in the **Near End Mask** box (255.255.255.255).

__ 8. Click the **Link Type** drop-down box to select **Numbered** or **Unnumbered**.

__ 9. Click the **TL Id** drop-down box to select the ID number for the TL (**1**–**1000**).

__ 10. (Optional) Type the resource class of the TL in the **Resource Class** box. (Double quoted four-byte hex string, for example, “3E04990A.”)

__ 11. Click the **Near End Parent TL** drop-down box to select the near end parent TL. The Near End Parent TL parameter identifies the TL to be used to specify an address for an unnumbered TL.

__ 12. (Optional) Type the carrier ID of the TL in the **Carrier ID** box. (1–30 character string enclosed in double quotes.)

__ 13. Click the **Signaling** box to enable signaling. Leave the box unchecked to disable signaling.

__ 14. Click the **Discovery** box to enable neighbor node discovery. Leave the box unchecked to disable neighbor node discovery.

Note: *Only INNI TLs are supported and a single area is exchanged in the Control Plane Hierarchy Negotiation (CPN) phase of neighbor discovery.*

__ 15. If necessary, type the neighbor node interface index in the **Interface Index** box.

__ 16. If necessary, type the ID of the neighbor node in the **Node ID** box.

__ 17. If necessary, type the neighbor node signaling address in the **Signaling Address** box.

__ 18. If necessary, type the neighbor node signaling ID in the **Signaling ID** box.

__ 19. In the **Link** area, click the **Cost** up and down arrows to set the Cost value (**1**–**4294967295**).

__ 20. Click the **Latency mode** drop-down box to select **MANUAL** (if the latency value will be manually provisioned) or **DISABLED** (if the latency parameter is not populated).

__ 21. If necessary, type the latency in the **Latency (ms)** box.

__ 22. Click the **Profile** drop-down box to select the link profile. (LINKPF-94 is the null profile).

__ 23. Click the **SRLG In Use** check box to enable SRLG.

__ 24. Type the SRLG value in the **SRLG** box.

__ 25. If necessary, in the **Routing** area, click the **Router Area Id** drop-down box to select the router area ID (for example, 100.1.2.1).

Note: *Within the MCN partition, the routing area ID (RAID) of a TL determines its function. The TL handles CP management communications if the RAID is configured to the same value as the management OSFP area. The TL handles CP signaling communications if the RAID is configured to the same value as the signaling OSPF area.*

__ 26. Click the **Routing Type** drop-down box to select **PASSIVE**, **ACTIVE**, or **DISABLED**.

__ 27. In the **Management Command** area, click **OOS (Out of Service)** or **IS (In Service)** to set the state of the TL.

__ 28. Click **OK**. The newly created TL displays in the **Topological Link** table.

Verifying OSPF Routing Adjacency

12.22 If you have created neighboring MCN partitions, the system creates an OSFP routing adjacency. If necessary, go to Managing OSPF Adjacency Properties, page 15-253 to verify the OSPF routing adjacency properties.

Creating TL for an Ethernet Signaling Port in the MCN

12.23 If necessary, create a TL for a signaling Ethernet port. Complete the procedure in Creating TL, page 15-242. The following are examples of signaling Ethernet port configurations for an mTera system running control plane:

- Create a NP-1 TL (TL-1-x-x), and provision its resource to one MGTETH interface on the SEIM module, such as MGTETH-20-21-3. Set the RAID of the TL equal to the **signaling** OPPF area.
- Create a NP-1 TL (TL-1-x-x), and provision its resource to one MGTETH interface on the SEIM module, such as MGTETH-20-21-4. Set the RAID of the TL equal to the **management** OPPF area.

Note: *Within the MCN partition, the routing area ID (RAID) of a TL determines its function. The TL handles CP management communications if the RAID is configured to the same value as the management OSFP area. The TL handles CP signaling communications if the RAID is configured to the same value as the signaling OSFP area.*

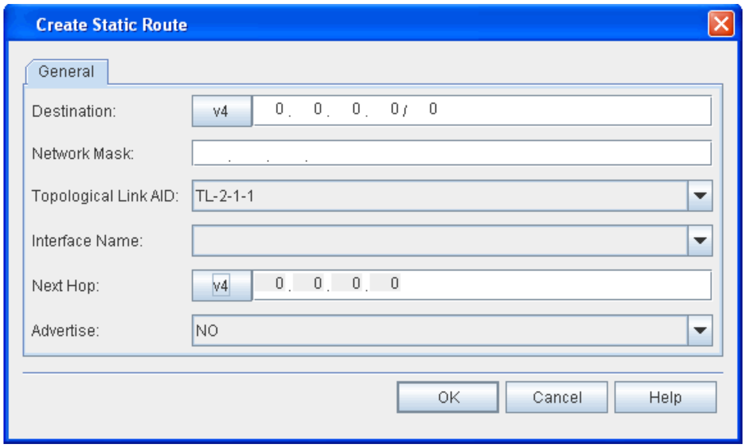
Creating Static Route

12.24 Create a static route to identify a static call path by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-1** icon to view the shortcut menu, then click **Routing**. The **Routing** tabbed view displays.

__ 2. Click the **Static Route** tab, then click **Create**. The **Create Static Route** dialog box displays. Refer to Figure 12.9, page 15-245.

Figure 12.9 Create Static Route



Create Static Route

General

Destination: v4 0 . 0 . 0 . 0 / 0

Network Mask: . . .

Topological Link AID: TL-2-1-1

Interface Name:

Next Hop: v4 0 . 0 . 0 . 0

Advertise: NO

__ 3. In the **Destination** box, type the IPv4 or IPv6 address of the call destination.

__ 4. In the **Network Mask** box, type the network mask.

__ 5. Click the **Topological Link AID** to select the TL to use in the static route.

Note: *If you select a TL for the static route, the Interface Name is not necessary.*

__ 6. Click the **Interface Name** drop-down box to select the TL AID for the static route (for example, an Ethernet port TL with a resource of MGTETH or IPPG.) The default value is none.

Note: *If you select an interface name for the static route, the Topological Link AID is not necessary.*

__ 7. In the **Next Hop** box, type the IPv4 or IPv6 address of the next hop of the call path.

__ 8. Click the **Advertise** drop-down box to select **YES** or **NO** to specify if the call path is advertised to the Control Plane network.

__ 9. Click **OK**. The newly created static route displays in the **Routing** dialog box.

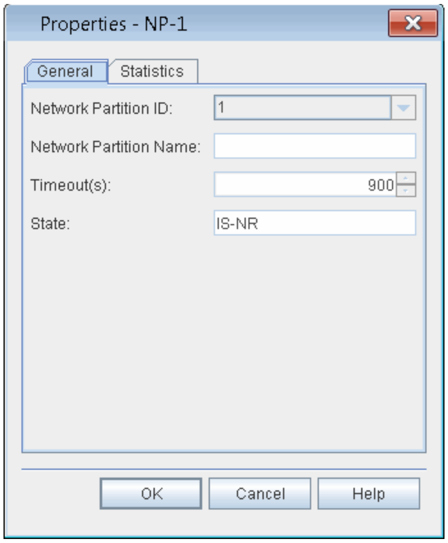
Network Partition Properties

12.25 View the properties of the MCN partition by performing the following steps:

Note: *The properties of the MCN partition are view-only.*

__ 1. In the **Navigation Window**, right-click the **NP-1** icon to view the shortcut menu, then click **Properties**. The **Properties - NP-x** dialog box displays. Refer to Figure 12.10, page 15-247.

Figure 12.10 Properties - NP-3(TPCP)



Network Partition ID: 1

Network Partition Name:

Timeout(s): 900

State: IS-NR

__ 2. In the **Network Partition Name** box, type a name for the network partition. (The network partition name can be up to 30 characters in length.)

__ 3. Click the **Timeout** drop-down box to select the default timeout for a call setup request (**10** seconds–**900** seconds.) The system defaults to 120 seconds.

__ 4. Click **OK**.

Managing Nodes

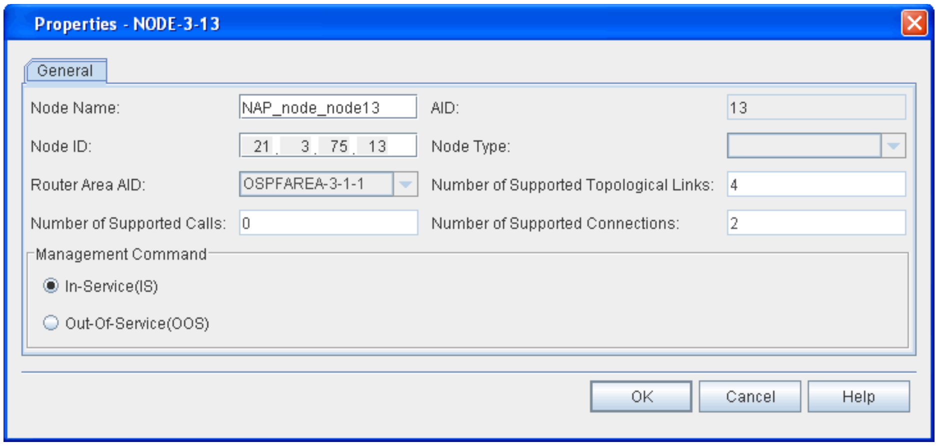
12.26 View or change the properties of a node by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-1** icon to view the shortcut menu, then click **Nodes and Links**. The **Nodes and Topological LInk** tabbed view displays.

__ 2. Highlight the node to select it.

__ 3. Click **Modify**. The **Properties - NODE-x-x** dialog box displays. Refer to Figure 12.11, page 15-248.

Figure 12.11 Properties - NODE-x-x



Properties - NODE-3-13

General

Node Name: NAP_node_node13

AID: 13

Node ID: 21 . 3 . 75 . 13

Node Type:

Router Area AID: OSPFAREA-3-1-1

Number of Supported Topological Links: 4

Number of Supported Calls: 0

Number of Supported Connections: 2

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

__ 4. (optional) In the **Node Name** box, type a name for the node (0–30 characters.)

__ 5. Verify the following information:

- **Node Type**
- **Router Area AID**

Note: *You can edit the Router Aid if the state of the node is OOS.*

- **Number of Supported Topological Links**
- **Number of Supported Calls**
- **Number of Supported Connections**

__ 6. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)** to set the state of the node.

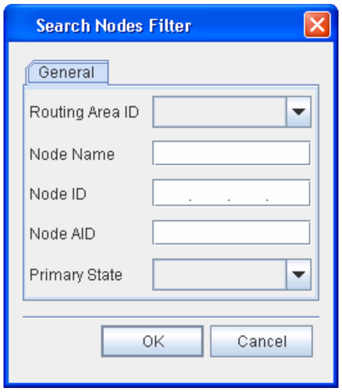
__ 7. Click **OK**.

Searching for Nodes

12.27 You can search for nodes by filtering on specified parameters. Search for a node by performing the following steps:

__ 1. In the **Nodes, Links, and TSL** tabbed view, click **Search**. The **Search Nodes Filter** dialog box displays. Refer to Figure 12.12, page 15-249.

Figure 12.12 Search Nodes Filter



Search Nodes Filter

General

Routing Area ID

Node Name

Node ID . . .

Node AID

Primary State

__ 2. Enter the available information in the dialog box to filter the node search based on the following parameters: **Routing Area ID**, **Node Name**, **Node ID**, **Node AID,** and **Primary State**.

__ 3. Click **OK**. Nodes that meet the filter criteria display in the **Node** table.

Managing TLs

12.28 View or change the properties of a topological link (TL) by performing the following steps:

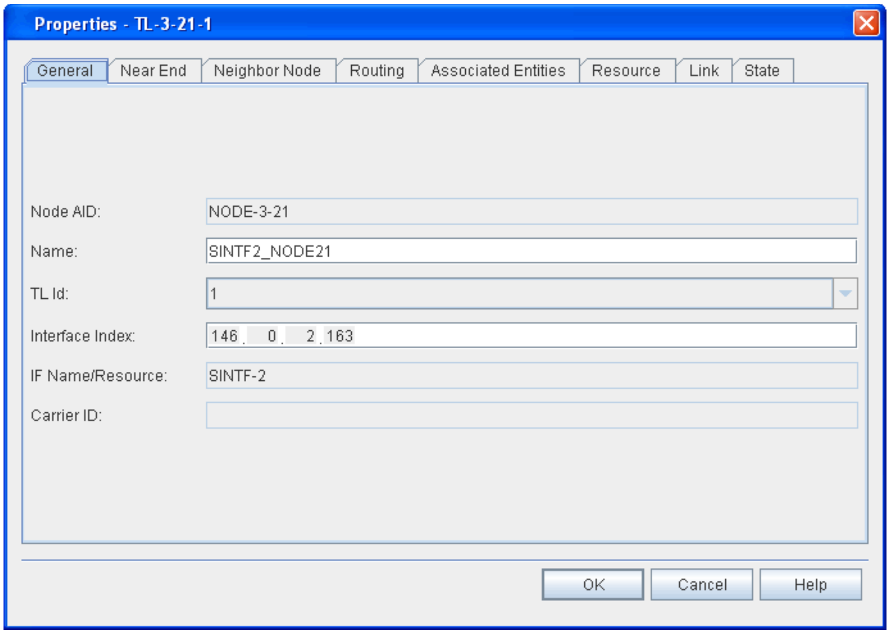
__ 1. In the **Navigation Window**, right-click the **NP-1** or **NP-3** icon to view the shortcut menu, then click **Nodes and Links**. The **Nodes, Links, and TSL** tabbed view displays.

__ 2. Click the **Topological Link** tab.

__ 3. Highlight the TL to select it.

__ 4. Click **Modify**. The **Properties - TL-x-x-x** dialog box displays. Refer to Figure 12.13, page 15-250.

Figure 12.13 Properties - TL-x-x-x



Node AID: NODE-3-21

Name: SINTF2_NODE21

TL Id: 1

Interface Index: 146 . 0 . 2 . 163

IF Name/Resource: SINTF-2

Carrier ID:

__ 5. Verify the **General** tab is selected.

__ 6. Verify the following information:

- **Node AID**
- (optional) type a name for the TL in the **Name** box
- **TL Id**
- **Interface Index**
- **IF Name/Resource**
- **Carrier ID**

__ 7. Click the **Near End** tab.

__ 8. Verify the following information:

- **Link Type**
- **Near End Address**
- **Near End Parent TL**
- **Near End Mask**

__ 9. Click the **Neighbor Node** tab.

__ 10. Verify the following information:

- **Discovery**
- **Signaling**

__ 11. If necessary, edit the following parameters:

- **Interface Index**
- **Node ID**
- **Signaling Address**
- **Signaling ID**

__ 12. Click the **Routing** tab.

__ 13. If necessary, edit the **Router Area Id**.

__ 14. Verify the **Router Area Id**.

__ 15. Click the **Routing Type** drop-down box to select **ACTIVE**, **PASSIVE**, or **DISABLED**.

__ 16. Click the **Associated Entities** tab.

__ 17. Verify the associated entities in the **Number of Entries in TNA Table** box.

__ 18. Click the **Resource** tab.

__ 19. Verify the following information:

- **Resource Aid**
- **Resource Class**

__ 20. Click the **Link** tab.

__ 21. If necessary, click the up- and down-arrows to configure the **Cost**.

__ 22. Click the **Latency Mode** drop-down box to select **Manual** or **Disabled**.

__ 23. Verify the following information:

- **Latency (ms)**
- **Profile**
- **SRLG in Use**
- **SRLG**

__ 24. Click the **State** tab.

__ 25. Verify the **Primary State**.

__ 26. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)** to set the state of the TL.

__ 27. Click **OK**.

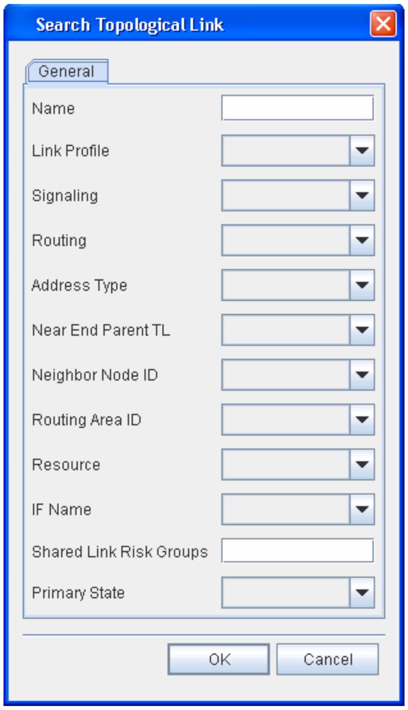
Searching for TLs

12.29 You can search for TLs by filtering on specified parameters. Search for a TL by performing the following steps:

__ 1. In the **Nodes, Links, and TSL** tabbed view, click the **Topological Link** tab.

__ 2. Click **Search**. The **Search Topological Link** dialog box displays. Refer to Figure 12.14, page 15-252.

Figure 12.14 Search Topological Link



__ 3. Enter the available information in the dialog box to filter the TL search based on the following parameters: **Name**, **Link Profile**, **Signaling**, **Routing**, **Address Type**, **Near End Parent TL**, **Neighbor Node ID**, **Routing Area ID**, **Resource**, **IF Name**, **Shared Link Risk Groups**, and **Primary State**.

__ 4. Click **OK**. TLs that meet the filter criteria display in the **Topological Link** table.

Managing Routing and Signaling Elements

12.30 For the MCN partition, you can view or change the properties of the OSPF Routing Controller, OSPF Adjacency, OSPF Area, Static Route, and Active Route from the Routing dialog box.

Managing OSPF Routing Controller Properties

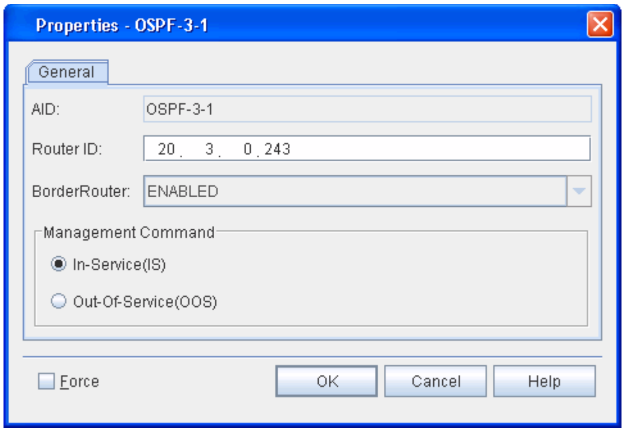
12.31 View or modify the properties of the OSPF Routing Controller for the MCN partition by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-1** or **NP-3** icon to view the shortcut menu, then click **Routing**. The **Routing** tabbed view displays.

__ 2. Click the **OSPF Routing Controller** tab.

__ 3. Click the OSPF routing controller instance to highlight it. Click **Modify**. The **Properties - OSPF-x-x** dialog box displays. Refer to Figure 12.15, page 15-253.

Figure 12.15 Properties - OSPF-x-x



Properties - OSPF-3-1

AID: OSPF-3-1

Router ID: 20 . 3 . 0 . 243

BorderRouter: ENABLED

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

□ Force

__ 4. Review the properties of the OSPF routing controller that display in the **AID**, **Router ID**, and **BorderRouter** fields.

__ 5. If necessary, type a new router address in the **Router ID** box.

__ 6. If necessary, change the primary state of the OSPF routing controller by clicking **OOS (Out Of Service)** or **IS (In Service)**.

__ 7. If you want to change the properties of the OSPF routing controller and override warning messages about affecting traffic, click **Force**.

__ 8. Click **OK**.

Managing OSPF Adjacency Properties

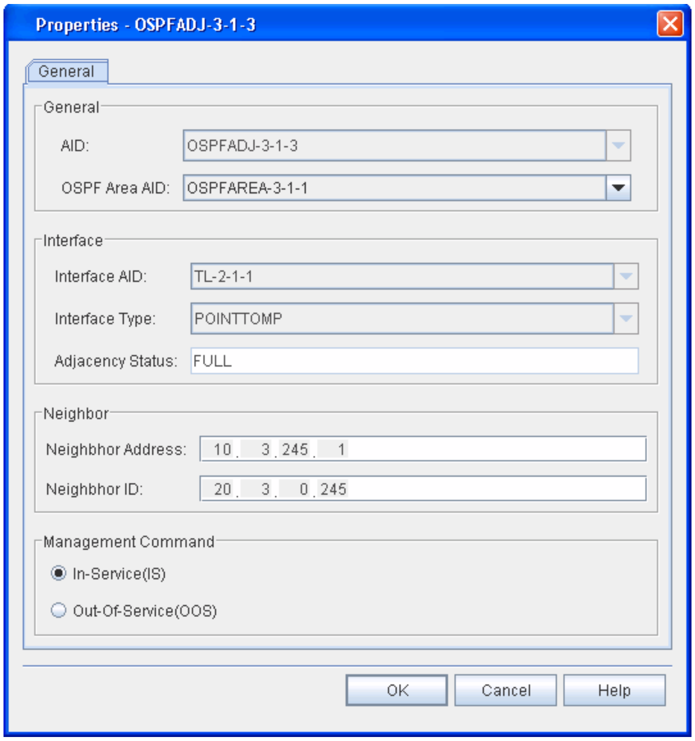
12.32 View or modify the properties of the OSPF Area for the MCN partition by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-1** or **NP-3** icon to view the shortcut menu, then click **Routing**. The **Routing** tabbed view displays.

__ 2. Click the **OSPF Adjacency** tab.

__ 3. Click the OSPFADJ-x-x-x instance to highlight it. Click **Modify**. The **Properties - OSPFADJ-x-x-x** dialog box displays. Refer to Figure 12.16, page 15-254.

Figure 12.16 Properties -OSPFADJ-x-x-x



Properties - OSPFADJ-3-1-3

General

General

AID: OSPFADJ-3-1-3

OSPF Area AID: OSPFAREA-3-1-1

Interface

Interface AID: TL-2-1-1

Interface Type: POINTTOMP

Adjacency Status: FULL

Neighbor

Neighbhor Address: 10 . 3 . 245 . 1

Neighbhor ID: 20 . 3 . 0 . 245

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

__ 4. If necessary, right-click the **OSPF Area AID** drop-down box to assign a new OSPF area to the OSPF adjacency.

__ 5. If necessary, click **IS (In Service)** or **OOS (Out of Service)** to change the primary state of the OSPF adjacency.

__ 6. Click **OK**.

Managing OSPF Area Properties

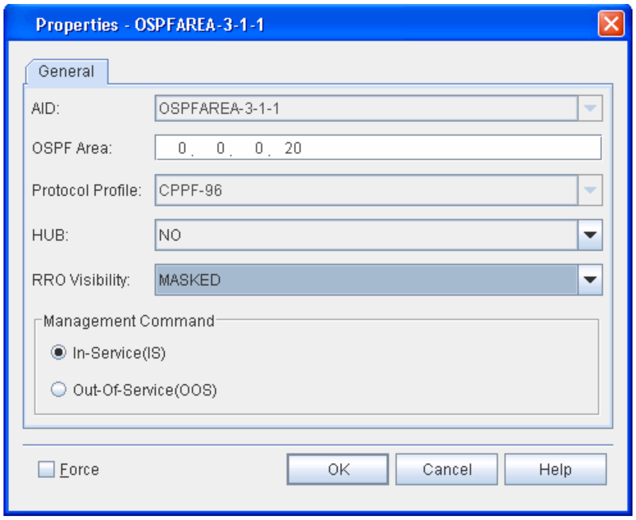
12.33 View or modify the properties of the OSPF Area for the MCN partition by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-1** or **NP-3** icon to view the shortcut menu, then click **Routing**. The **Routing** tabbed view displays.

__ 2. Click the **OSPF Area** tab.

__ 3. Highlight the OSPFAREA entity to select it. Click **Modify**. The **Properties - OSPFAREA-x-x-x** dialog box displays. Refer to Figure 12.17, page 15-255.

Figure 12.17 Properties - OSPFAREA-x-x-x



Properties - OSPFAREA-3-1-1

General

AID: OSPFAREA-3-1-1

OSPF Area: 0 . 0 . 0 . 20

Protocol Profile: CPPF-96

HUB: NO

RRO Visibility: MASKED

Management Command

● In-Service(IS)

○ Out-Of-Service(OOS)

□ Force

__ 4. Review the properties of the OSPFAREA display in the **AID**, **OSPF Area**, and **Protocol Profile** fields.

__ 5. Click the **HUB** drop-down box to select **YES** (if the OSPF area is a hub) or **NO** (if the OSPF area is not a hub).

__ 6. Click the **RRO Visibility** drop-down box to select **PASSED** (recorded route object for this area is to be propagated outside of the area as well as within the area) or **MASKED** (recorded route object for this area is to be propagated within the area but not to be propagated outside of the area).

__ 7. In the **Management Command** area, click **In-Service(IS)** or **Out-Of-Service(OOS)** to set the state of the entity.

__ 8. If you want to change the state of the OSPFAREA and override warning messages about affecting traffic, click **Force**.

__ 9. Click **OK** to save the changes and close the dialog box.

Managing Static Route (NP-1)

12.34 View or modify the properties of an static route by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-1** icon to view the shortcut menu, then click **Routing**. The **Routing** tabbed view displays.

__ 2. Click the **Static Route** tab.

__ 3. Click the static route instance to highlight it. Click **Modify**. The **Properties - Static Route** dialog box displays.

__ 4. Review the static route properties.

__ 5. Click **Cancel** to close the dialog box.

Managing Active Route (NP-1)

12.35 View a list of active routes by performing the following steps:

__ 1. In the **Navigation Window**, right-click the **NP-1** icon to view the shortcut menu, then click **Routing**. The **Routing** tabbed view displays.

__ 2. Click the **Active Route** tab.

__ 3. Click **Refresh** to update the list of active routes.

__ 4. Click **Close**.

Index

USER NOTES