OnSite 1052 &1063 Series
Metro-Optical Transport Access Nodes

Administrator's Reference Guide

Sales Office: **+1 (301) 975-1000**
Technical Support: **+1 (301) 975-1007**
E-mail: **support@patton.com**
WWW: **www.patton.com**

Part Number: **07MOS10xx-ARG, Rev. B**
Revised: **February 21, 2012**

Patton Electronics Company, Inc.
7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
Tel: +1 (301) 975-1000
Fax: +1 (301) 869-9293
Support: +1 (301) 975-1007
Web: www.patton.com
E-mail: support@patton.com

The information in this document is subject to change without notice. Patton Electronics assumes no liability for errors that may appear in this document.

Summary Table of Contents

Table of Contents

List of Figures

List of Tables

About this guide

This guide describes how to configure and manage a Patton OnSite Series Model 1052 and1063 Metro-Optical Transport Access Node. For detailed installation instructions, refer to the *OnSite 1052 & 1063 Series User Manual*, available online at **www.patton.com/manuals/OS10xx.pdf**.

Installation, maintenance, and removal of a chassis or its components must be done by qualified service personnel only. Qualified service personnel have had appropriate technical training and experience that is necessary to be aware of the hazards to which they are exposed when performing a task and of measures to minimize the danger to themselves and other people.

You should consider the following before unpacking your equipment:

- Install the equipment in a secured, enclosed, and restricted access area, ensuring that only qualified service personnel have access to the equipment.
- Install the equipment only in a temperature and humidity-controlled indoor area that is free of airborne materials that can conduct electricity.
- When you handle equipment that has expansion modules, put on the electrostatic discharge (ESD) wrist strap to reduce the risk of electronic damage to the equipment.

Note Leave the ESD strap permanently attached to the chassis or rack so that it is always available when you need to handle ESD-sensitive components.

WARNING **Read the following safety information thoroughly before installing your OS-10 system. Failure to follow this safety information can lead to personal injury or damage to the equipment.**

Audience

This guide is intended for the following users:

- Operators
- Installers
- Maintenance technicians

Structure

This guide contains the following chapters and appendices:

- Chapter 1 describes how to access and manage the system
- Chapter 2 describes how to get started configuring the system
- Chapter 3 describes how to configure and manage the STM-1 interface
- Chapter 4 describes how to configure and manage the E1/T1 interface
- Chapter 5 describes how to configure and manage the DS3/E3 interface
- Chapter 6 describes how to configure and manage the Ethernet interface
- Chapter 7 describes how to install the high-density E1 expansion module
- Chapter 8 describes how to install the high-density Ethernet expansion module
- Chapter 9 describes how to install the high-density DS3/E3 expansion module
- Chapter 10 describes how to install the STM-1 expansion module
- Chapter 11 contains information on contacting Patton technical support for assistance
- Appendix A contains a reference for terms and acronyms found in this guide

For best results, read the contents of this guide *before* you install and configure the OS-10 platforms.

Precautions

Notes and cautions, which have the following meanings, are used throughout this guide to help you become aware of potential problems. *Warnings* relate to personal injury issues, and *Cautions* refer to potential property damage.

Note Calls attention to important information.

WARNING

The shock hazard symbol and WARNING heading indicate a potential electric shock hazard. Strictly follow the warning instructions to avoid injury caused by electric shock.

WARNING

The alert symbol and WARNING heading indicate a potential safety hazard. Strictly follow the warning instructions to avoid personal injury.

CAUTION

The shock hazard symbol and CAUTION heading indicate a potential electric shock hazard. Strictly follow the instructions to avoid property damage caused by electric shock.

CAUTION

The alert symbol and CAUTION heading indicate a potential hazard. Strictly follow the instructions to avoid property damage.

Typographical conventions used in this document

This section describes the typographical conventions and terms used in this guide.

General conventions

The procedures described in this manual use the following text conventions:

Table 1. General conventions

Convention	Meaning
Garamond blue type	Indicates a cross-reference hyperlink that points to a figure, graphic, table, or section heading. Clicking on the hyperlink jumps you to the reference. When you have finished reviewing the reference, click on the **Go to Previous View** button in the Adobe® Acrobat® Reader toolbar to return to your starting point.
Futura bold type	Indicates the names of menu bar options.
Italicized Futura type	Indicates the names of options on pull-down menus.
Futura type	Indicates the names of fields or windows.
Garamond bold type	Indicates the names of command buttons that execute an action.
< >	Angle brackets indicate function and keyboard keys, such as **<Shift>**, **<Ctrl>**, **<C>**, and so on.
`Are you ready?`	All system messages and prompts appear in the `Courier` font as the system would display them.
`% dir *.*`	Bold Courier font indicates where the operator must type a response or command

Mouse conventions

The following conventions are used when describing mouse actions:

Table 2. Mouse conventions

Convention	Meaning
Left mouse button	This button refers to the primary or leftmost mouse button (unless you have changed the default configuration).
Right mouse button	This button refers the secondary or rightmost mouse button (unless you have changed the default configuration).
Point	This word means to move the mouse in such a way that the tip of the pointing arrow on the screen ends up resting at the desired location.
Click	Means to quickly press and release the left or right mouse button (as instructed in the procedure). Make sure you do not move the mouse pointer while clicking a mouse button.
Double-click	Means to press and release the same mouse button two times quickly
Drag	This word means to point the arrow and then hold down the left or right mouse button (as instructed in the procedure) as you move the mouse to a new location. When you have moved the mouse pointer to the desired location, you can release the mouse button.

Safety when using electricity

⚠ WARNING

Read the installation instructions before connecting your OS-10 system to the power source.

Follow these guidelines when working on equipment powered by electricity:

- Locate the emergency power-off switch in the room in which you are working. Then, if an electrical accident occurs, you can quickly turn off the power.
- Never assume that power is disconnected from a circuit. Disconnect all power before installing or removing a chassis or working near power supplies.
- Ground the unit. Do not connect the power supply unit to an AC outlet without a ground connection.
- Connect the unit to a grounded AC outlet to comply with the appropriate regional safety standards.
- Place the unit near the socket outlet to be easily accessible.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- Do not work alone if hazardous conditions exist.

In addition, following these guidelines when working on any equipment that is disconnected from a power source but still connected to telephone wiring or other network cabling:

- Never install telephone wiring during a lightning storm.
- Never touch uninsulated telephone wires or terminals unless the telephone line is disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

Power Cable

If your system comes with the AC power option, use an AC power cable appropriate for your country.

Check your local electrical codes and regulatory agencies for power cable requirements.

Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. It can occur if electronic printed circuit cards are improperly handled and can cause complete or intermittent failures. Always follow these ESD prevention procedures when removing and replacing expansion modules:

- Ensure that the system chassis is electrically connected to earth ground.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame or to the rack to channel unwanted ESD voltages safely to ground. To guard against ESD damage and shocks, the wrist strap and cord must operate effectively.
- If no wrist strap is available, ground yourself by touching an unpainted metal part of the chassis or rack.

CAUTION

To prevent equipment damage because of ESD, periodically check the resistance value of the antistatic strap. It should be between 1 and 10 M¾ (Mohm).

Optical Safety

WARNING

Use fiber-optic ports only for telecommunications applications that require optical fiber. Use the ports only with the appropriate connector. When not in use, replace the dust covers. Using these interfaces in ways other than those described in this guide can cause property damage or personal injury.

Fiber-Optic Ports

To protect your eyes, never look at the transmit LED or laser through a magnifying device while it is powered on. Never look directly at a fiber port on the chassis or at the ends of fiber cable when they are powered on.

Note The OS-10 system uses a CLASS 1 laser device.

Fiber-Optic Safety Precautions

Follow these safety precautions when working with fiber-optic cables:

- Do not eat, drink or smoke in the work area. If fiber particles are ingested they could cause internal hemorrhaging.
- Wear safety glasses with side shields to avoid getting fiber-optic splinters in your eyes.
- Do not look into the end of a fiber cable until you are sure that there is no light source at the other end. Use a fiber-optic power meter to ensure that the fiber is dark (that is, no power is being carried).
- Ensure that the work area is well ventilated.
- Do not touch your eyes while working with fiber-optic cables.
- Wear disposable aprons to minimize fiber particles on your clothing.
- Dispose of all cut fiber-optic pieces properly.
- Thoroughly clean the work area when the installation is complete.

Chapter 1 System Management Access

Chapter contents

Introduction

This chapter provides the procedures for configuring and monitoring the local serial and LAN management (LM) ports, and the inband management channel (IMC) for remote management communications. The chapter also provides the procedures for configuring and using the Orderwire communications port (if the AUX port is factory-installed).

General Overview

The base OnSite OS-10 system provides two management ports from which you can access the system management functions. One of the management ports is an Ethernet LAN (10/100BASE-TX) port. The other is an RS-232 SERIAL port.

figure 1 shows the location of the two management ports on the base OS1052 and OS1063 systems.

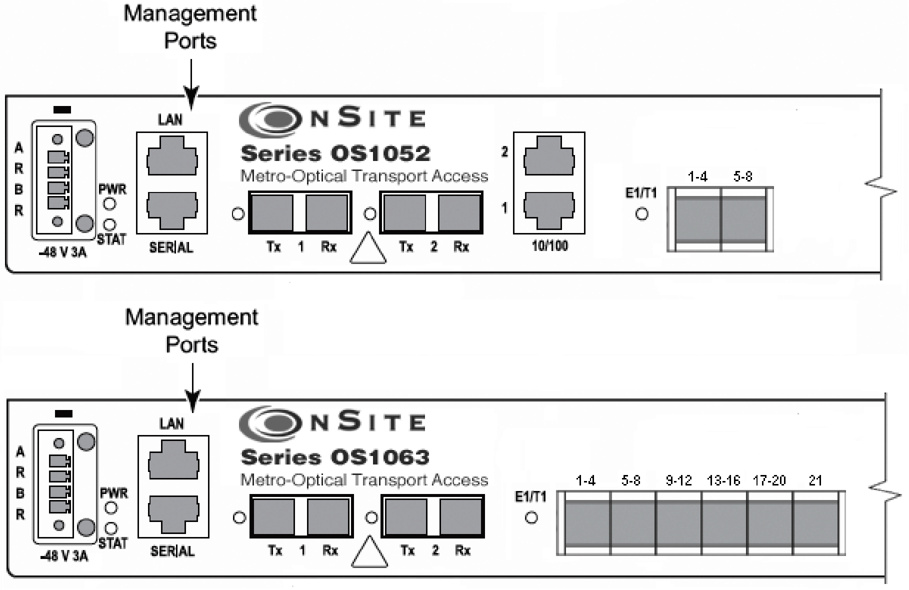


Figure 1. Serial and LAN Management Ports on the Base OS1052 and OS1063 Systems

figure 2 provides a close-up view of the two management ports. The figure includes the location of the RJ-45 connector pins for both ports.

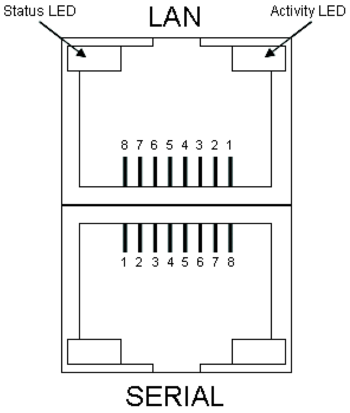


Figure 2. Detail of the Management Ports

figure 3 shows the location of the signal pins on the RJ-45 plug.

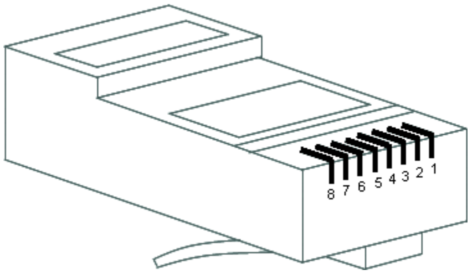


Figure 3. Location of Signal Pins on the RJ-45 Plug

Ethernet LAN Management Port

The Ethernet LAN management port complies with the following standards:

- IEEE 802.3u (PHY)
- IEEE 802.3 (MAC)
- IEEE 802.3x (flow control)

The port supports autonegotiation, which is always enabled.

table 3 provides the cabling specifications for the Ethernet LAN management port.

Table 3. Ethernet LAN Management Port Cabling Specifications

Cable	Specification
Connector	RJ-45
Type	Category 5
Reach	100 m

table 4 provides the pin assignments for the RJ-45 connector.

Table 4. Pin Assignments for the Ethernet LAN Management Port

Signal Name	Description	RJ-45 Pin
RXN	Receive tip	3
RXP	Receive ring	6
TXN	Transmit tip	1
TXP	Transmit ring	2

Serial Management Port

The physical connector for the RS-232 SERIAL management port is an RJ-45 connector. table 5 provides the pin assignments for the RJ-45 connector.

Note A connector adapter is supplied with the system to allow the connection of the RS-232 signal to a PC with a DB-9 connector.

Table 5. Pin Assignments for the RS-232 Serial Management Port

Signal Name	Description	RJ-45 Pin
RS232_TXD output	Transmit data	6
RS232_RXD input	Receive data	3
GND	Ground	4 and 5

table 6 lists the serial port parameters:

Table 6. RS-232 Serial Port Parameters

Parameter	Property
Baud rate	9,600 to 38,400 (asynchronous)
Data	8 bits
Parity	None
Stop	1 bit

table 7 lists the required VT100 terminal emulation settings for the PC that connects to the serial port.

Table 7. VT100 Terminal Emulation Settings

Parameter	Setting
Port	COM1
Baud rate	9,600
Data	8 bits
Parity	None
Stop	1 bit
Flow control	None

Gaining Access to the System

There are two ways of gaining access to the system management functions. One way is through the SERIAL port and the command line interface (CLI). The other way is through the Ethernet LAN port and the web browser interface. The following sections describe the procedures for each of the access methods.

Access through the Serial Port

To gain management access to the system for the first time through the SERIAL port, follow these steps:

1. Connect a PC to the SERIAL management port.

   Note Use the DB-9-to-RJ-45 adapter cable supplied with the system.

2. Launch the VT100 terminal emulation program on the PC.

   Note Configure the terminal in accordance with the settings in Table 14.

3. Press the Enter key on the PC to obtain a login prompt from the system.
4. Log in to the system using the Super user ID and password.

   Note Only the Super user is able to perform the following task.

   Note The user ID for the Super user is super (all lowercase letters).

   Note The factory-assigned default password for the Super user is super (all lowercase letters).

   After successful completion of the login, the system responds with the CLI (command-line interface) prompt.

   Note The CLI command prompt for the system is OnSite >

5. Type the following CLI command to configure the IP address for the Ethernet LAN management port, and then press the Enter key:

   ```
   config mgmt-enet ip-address aaa.bbb.ccc.ddd
   ```

   Note aaa.bbb.ccc.ddd is the standard dotted-decimal notation.

6. Type the following CLI command to configure the net mask for the Ethernet LAN management port, and then press the Enter key:

   ```
   config mgmt-enet ip-netmask aaa.bbb.ccc.ddd
   ```

7. Type the following CLI command to configure the default gateway for the Ethernet LANmanagement port, and then press the Enter key:

   ```
   config mgmt-enet default-gateway aaa.bbb.ccc.ddd
   ```

   Note By default, the IP address is set to 192.168.2.100, the net mask is set to 255.255.255.0, and the default gateway is set to 192.168.2.1

8. Type the following CLI command to save the IP settings (address, net mask, and default gateway)for the Ethernet LAN management port to the system configuration file, and then press the Enter key:

```
save config
```

Note Saving the configuration is important to prevent the loss of the IP configuration data if a system reset or reboot occurs.

CAUTION

Changing the IP address, net mask, and default gateway settings for the Ethernet LAN management port could result in the loss-of-management connectivity to the system, if the connection is currently through that port.

At this point, the system responds with Configuration Saved to indicate that the IP settings have been saved to the system. The system is now ready for operation using the Web-based management interface.

Note You may also have access to the system through Telnet. This access requires prior configuration of the IP address of the Ethernet LAN management port through the RS-232 SERIAL port, as indicated in the preceding steps.

Note The system terminates the management session for any user when the session remains inactive for 30 seconds. This termination applies to management sessions through the SERIAL port or through Telnet. The login prompt appears when the system terminates a previously active session through the SERIAL port.

Access through the Ethernet LAN Management Port

To gain management access to the system for the first time through the Ethernet LAN management (LM) port, follow these steps:

1. Connect a PC to the Ethernet LAN management port using the RJ-45 connector.

Note You may connect the PC to the system from a remote location using an IP LAN or WAN that connects to the Ethernet LAN management port.

2. Configure the PC using the factory default settings for the Ethernet LAN management port.

Note By default, the IP address is set to 192.168.2.100, the net mask is set to 255.255.255.0, and the default gateway is set to 192.168.2.1

3. Launch the Web browser of your choice, and type the default IP address of the system in the Address field of the browser.

4. Log in to the system using the super, admin, or monitor user ID and password.

Note The factory-assigned default password for the Super user is super (all lowercase letters).

See “Web-Based Management Interface” on page 27 for a description of the Web-based management interface features. Once you gain access to the system through the Ethernet LAN port, you may change the IP settings for the port for secure access in the future.

CAUTION

Save the system configuration to prevent the loss of the new IP settings if a system reboot occurs.

Note Once the changes take place, you will loose connectivity to the system, but you can regain access immediately by typing the new IP address of the system in the Address field of the browser.

Web-Based Management Interface

The system provides a simple but powerful Web-based management interface to configure and monitor the OnSite OS-10 system. This graphical user interface (GUI) is called the OnSight Device Manager (DM) and is accessible through a Web browser using Hypertext Transfer Protocol (HTTP).

Note The system supports the following Web browsers: Microsoft Internet Explorer 6+, Netscape 7+, Mozilla 1.7+, and Mozilla Firefox 1.0+ on Windows, Solaris, and Linux platforms.

The OnSight DM allows you to have full access to the system management functions. These functions include the ability to set up or change all configurable items on the system and the ability to create and delete connections between the client ports and SDH network interface. The interface also allows you to monitor and display current active alarms, performance monitoring parameters, and alarm and event logs.

Launching the GUI Application

To launch the Web-based management interface, follow these steps:

Note This procedure requires prior configuration of the IP address of the Ethernet LAN management port through the RS-232 SERIAL port or LAN port, as indicated in §6.4.

1. Connect the PC to the Ethernet LAN management port using the RJ-45 connector.

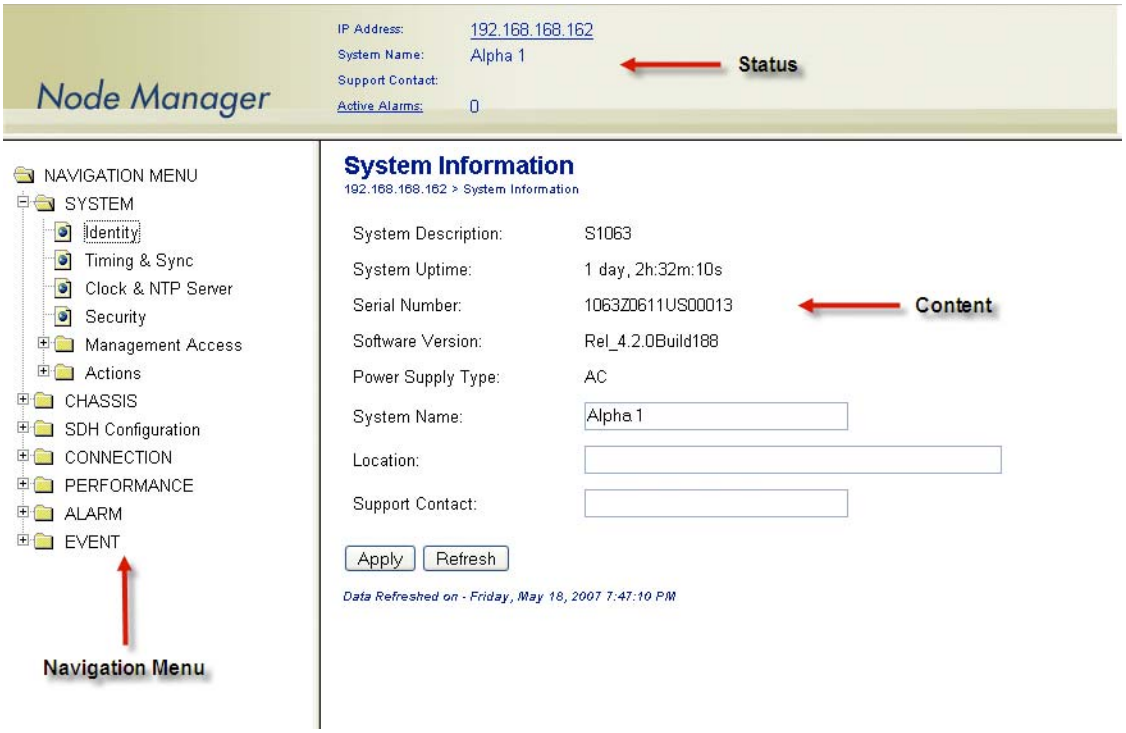
Note You may connect the PC to the system from a remote location using an IP LAN or WAN that connects to the Ethernet LAN management port.

2. Launch the Web browser of your choice, and type the IP address of the system in the Address field of the browser.
3. Log in to the system using the **super**, **admin**, or **monitor** user ID and password.

After successful completion of the login, the browser displays the OnSight DM splash screen from which you can select the language of your choice (English or Chinese, currently). After language selection, the browser displays the **System Information** page. The OnSight DM screen is divided into three frames, as shown in figure 4. table 8 provides a description of each frame.

You may now start to configure and operate the system using the GUI interface.

Note For proper display of the GUI interface, you must set your browser to allow "pop-up" windows.


Node Manager

IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Status

System Information
192.168.168.162 > System Information

System Description: S1063
System Uptime: 1 day, 2h:32m:10s
Serial Number: 1063Z0611US00013
Software Version: Rel_4.2.0Build188
Power Supply Type: AC
System Name: Alpha 1
Location:
Support Contact:

Content

Data Refreshed on - Friday, May 18, 2007 7:47:10 PM

Navigation Menu

Figure 4. Web-Based Management GUI Frames

Table 8. Web-Based Management GUI Frame Descriptions

GUI Frames	Provides...
Status (top frame)	An overview of the system identity, including the system name and IP address, and the support contact information and status of active alarms.
Navigation (bottom left frame)	The main categories and subdivisions of system functions.
Content (bottom right frame)	The main area for information display and configuration.

Autonomous Alarm Messages

You can configure the system to generate autonomous alarm messages that can be received and displayed by an SNMP-based network management system (NMS).

By default, the system does not generate SNMP traps. To allow the generation of SNMP traps, you must first configure the IP address of the NMS host device or devices to which you wish to direct the traps.

To configure the system as an SNMP trap sender for an SNMP trap receiver, see Figure 12 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Management Access**.
3. From the expanded **Management Access** folder, select **Trap Receiver.**
4. On the **SNMP Trap Receivers** page, click on **Add**.
5. In the **Add New Trap Receiver** page, type the **Trap Receiver Address** and **Community String**.

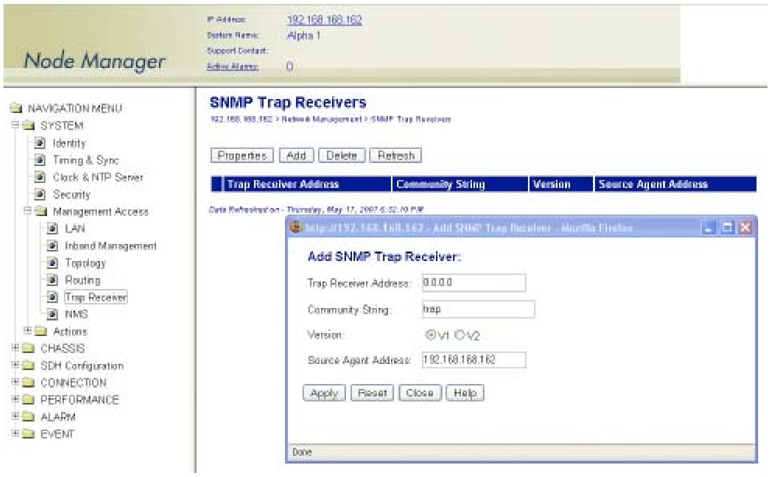
> **Note** The community string controls access between a client (the OS-10 system) and a server (the NMS host).

6. Set the **Version** to configure the system to send SNMP **V1** or **V2** traps.
7. Type the **Source Agent Address** of the SNMP agent.

> **Note** The OS-10 generates SNMP traps that contain the IP address of the source agent. By default, the system uses the address of the Ethernet LAN management port as the source agent address. However, you may use another address (for example, the inband management channel address) according to the routing settings for the system.

8. Click on **Close** to close the window.

At this point, the **Trap Receivers** page displays the settings for the new receiver.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

SNMP Trap Receivers

192.168.168.162 > Network Management > SNMP Trap Receivers

Trap Receiver Address	Community String	Version	Source Agent Address

Data Refreshed on - Thursday, May 17, 2007 6:32:10 PM

http://192.168.168.162 - Add SNMP Trap Receiver - Mozilla Firefox

Add SNMP Trap Receiver:

Trap Receiver Address: 0.0.0.0

Community String: trap

Version: ● V1 ○ V2

Source Agent Address: 192.168.168.162

Done

Figure 5. Configuring an SNMP Trap Receiver

To remove an existing SNMP trap receiver, follow these steps:

1. Select a trap receiver on the **SNMP Trap Receivers** page.
2. Click on **Delete** to remove the trap receiver.

At this point, the system removes the trap receiver, and it is no longer displayed in the table.

In addition to supporting the generation of traps to an SNMP-based NMS, the system also sends autonomous messages to all connected OnSight NMSs. The OnSight NMS provides centralized management and control of OS-10 systems in point-to-point, linear, and ring ADM subnetworks.

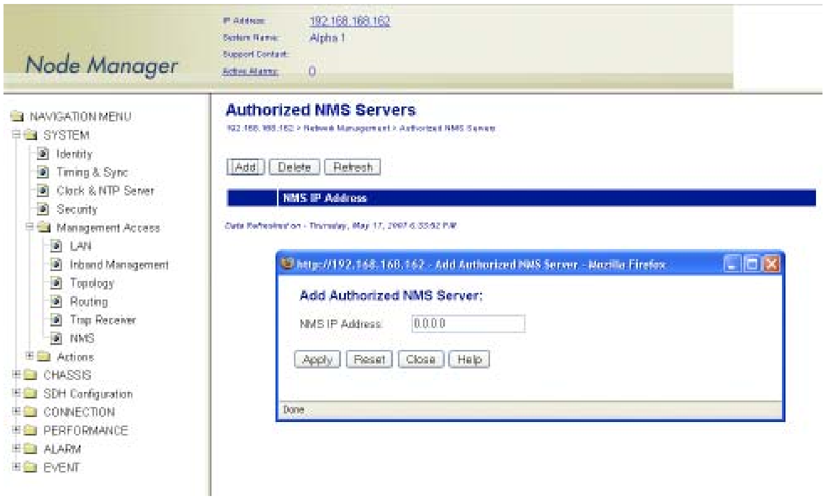
To display the OnSight NMS servers authorized to manage the OS-10 system, see figure 6 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Management Access**.
3. From the expanded **Management Access** folder, select **NMS**.

On the **Authorized NMS Servers** page, the table displays the IP addresses of the OnSight NMS servers authorized for management connectivity to the system.

To add an OnSight NMS server to the list of authorized servers, see figure 6 and follow these steps:

1. On the **Authorized NMS Servers** page, click on **Add**.
2. In the **Add Authorized NMS Server** window, type the **NMS IP Address** and click on **Apply**.
3. Click on **Close** to close the window.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Authorized NMS Servers

192.168.168.162 > Network Management > Authorized NMS Servers

Data Refreshed on - Thursday, May 17, 2007 6:33:52 PM

http://192.168.168.162 - Add Authorized NMS Server - Mozilla Firefox

Add Authorized NMS Server:

NMS IP Address: 0.0.0.0

Figure 6. Configuring an Authorized OnSight NMS Server

Engineering Orderwire (EOW)

If the system is equipped with the factory-installed AUX (auxiliary) board, you can use AUX port 1 (AUX 1) for voice communications between two or more interconnected OnSite OS-10 Series systems.

figure 7 shows the location of EOW port (AUX 1) on the system. The port is located on the right side of the chassis, at the back.

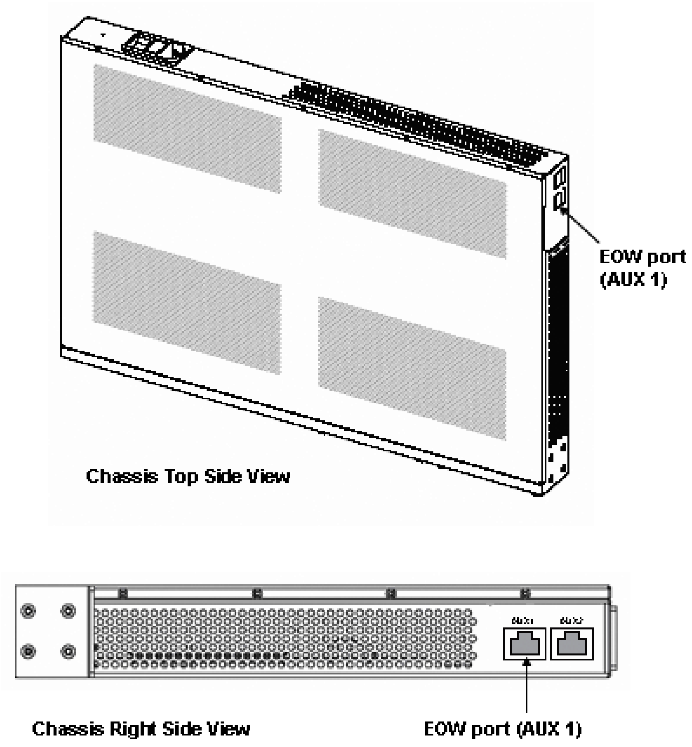


Figure 7. Location of EOW port (AUX 1) on OS-10 Series Chassis

The EOW port supports a 2-wire analog interface (tip and ring) with a nominal impedance of 900-ohm and A-law PCM voice encoding. The system carries the PCM-encoded 64 kbit/s voice channel in either the E1 or E2 byte of the STM-1 section overheard (SOH).

As a Foreign eXchange Station (FXS) interface, the EOW port supports the following functions:

- Dial tone
- Battery current
- Ring voltage

The system uses an RJ-11 connector for the EOW port (AUX 1) but only two pins are used for the 2-wire connection: pin 2 (tip) and pin 3 (ring), as shown in figure 8.

Note The "tip" is the ground side and the "ring" is the battery side of the 2-wire telephone circuit.

WARNING

To prevent electrical shock, never touch uninsulated wires or terminals when the phone line is plugged into the RJ-11 connector of the EOW port (AUX 1).

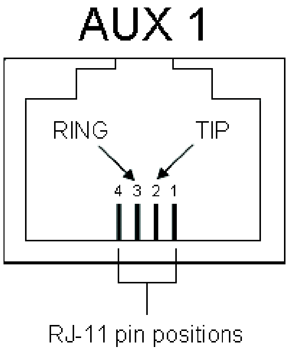


Figure 8. Location of signal pins on the EOW port (AUX 1) RJ-11 connector

The EOW port supports dual-tone multifrequency (DTMF) signaling to identify EOW stations within an OnSite OS-10 subnetwork. Each EOW station is identified with a programmable 3-digit station ID number.

To configure the engineering orderwire (EOW) function, see Figure 16 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Management Access**.
3. From the expanded **Management Access** folder, select **Orderwire**.

Note If you see that the physical connector for the AUX 1 port is present but the **Orderwire** selection does not appear on the folder, check first that the system is operating using Release 4.3 or above.

4. On the **Orderwire** page, check that the **AUX Board** shows Installed and that the **Operational Status** is in-service (**IS**).

Note If the AUX Board shows **Not Installed** or the **Operational Status** is out-of-service (**OOS**), and you see that the physical connector for the AUX1 port is present, contact your local systems engineer or regional OnSite support center for additional technical information.

5. On the **Orderwire** page, set the **Station ID** for the system.

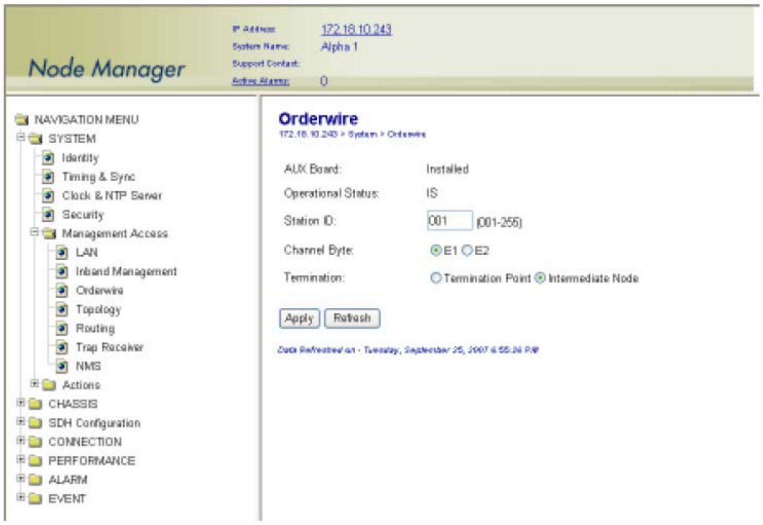
Note The Station ID needs to be a unique 3-digit number for each EOW station within an OnSite subnetwork. The available range of station ID numbers is 001 to 255.

Note In addition to supporting selective calling of EOW stations using the station ID, the EOW also supports a party-line function that allows calling and communicating with all EOW stations at once (party-line function) by dialing *000.

6. Set the **Channel Byte** to **E2** (express orderwire byte) if there are SDH regenerators present between the STM-1 ports connecting two OnSite OS-10 nodes supporting the EOW function; otherwise, leave the default setting as E1 (local orderwire byte).
7. Set **Termination** to **Termination Point** if the EOW station is an OS-10 node in terminal mux configuration in a point-to-point link or at the end of a linear ADM chain. For OS-10 nodes in ADM configuration, leave the default setting as **Intermediate Point**.

Note For OS-10 nodes in a ring network, one of the nodes must be set to **Termination Point** while the rest of the nodes are set to **Intermediate Point**. This arrangement is necessary to prevent an audio feedback loop. Normally, the OS-10 node serving as the master timing node for the ring is set to **Termination Point**.

8. Click on **Apply** to complete the configuration of the EOW port.



IP Address: 172.18.10.243
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Orderwire
172.18.10.243 > System > Orderwire

AUX Board: Installed
Operational Status: IS
Station ID: 001 (001-255)
Channel Byte: ● E1 ○ E2
Termination: ○ Termination Point ● Intermediate Node

Data Refreshed on - Tuesday, September 25, 2007 4:55:26 PM

Figure 9. Configuring the Engineering Orderwire (EOW) Function

After the EOW port is configured for operation, you can connect a regular 2-wire touchtone telephone set to the RJ-11 connector of the port. To establish a voice call with another EOW station on the same OnSite OS-10 subnetwork, take the phone "off-hook", wait for dial tone, and then dial star (*) followed by the Station ID number. For example, to call Station ID number 123, dial *123.

Note To use the EOW function, all OS-10 nodes in the subnetwork must be equipped with the factory-installed AUX board option. The nodes must also be configured with a unique station ID number for each node.

At this point, the called station begins to ring if another telephone set is connected to the EOW port of that station.

Note To call and communicate with all EOW stations at once (party-line function), dial *000.

To complete the call, simply place the telephone set in the on-hook position, like a regular analog phone.

Chapter 2 **System Configuration**

Chapter contents

Introduction

This chapter provides the procedures for configuring the global system attributes. These attributes include the system identity and IP settings for management communications using the local and inband management channels. It also provides procedures for configuring the system timing and synchronization functions and setting up the system clock. The chapter concludes with procedures for upgrading the system software, rebooting and resetting the system defaults, and transferring configuration and log files between the system and a remote server.

System Identity

To configure the system identity, see Figure 17 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Identity**.
3. On the **System Information** page, type the **System Name**, **Location**, and **Support Contact**.

> **Note** In **Location**, type the location of the system by using a physical address or any other network-specific site notation. Leave this field empty, if desired.

> **Note** In **System Name**, type any suitable name that identifies the system. Leave this field empty, if desired. The **System Name** appears on the Status frame at the top of the browser page.

> **Note** In **Support Contact**, type the e-mail address of the nearest support center or systems engineer servicing the system. Leave this field empty if desired. The **Support Contact** appears on the Status frame at the top of the browser page. When you click on the e-mail address, your email application opens a new message window to allow sending a message to your support contact.

> **Note** You may use up to 100 characters for the **Location**, **System Name** and **Support Contact**. The string can contain only the following alphanumeric characters: lower case letters (a through z), upper case letters (A through Z), numbers (0 through 9), hyphens (-), commas (,), colons (:), underscores (_), slashes (/), periods (.), spaces, parentheses, and the @ character.

4. Click on **Apply** to complete this task.

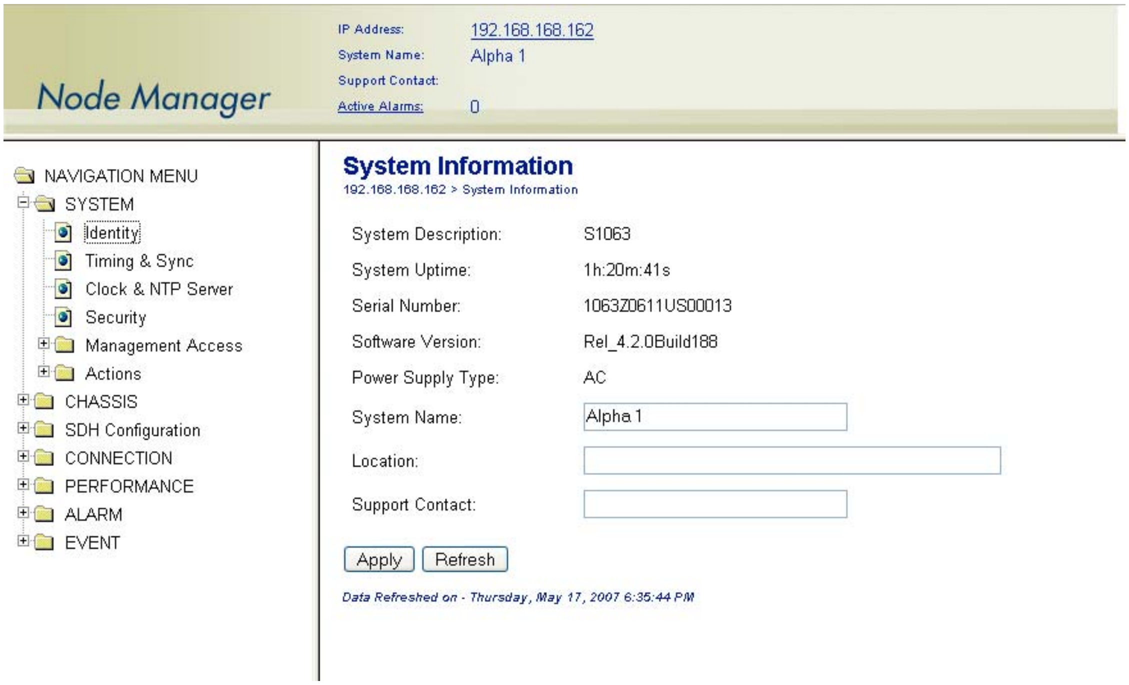
Table 9 on page 37 provides a description of all fields on the system information page.

Table 9. Description of Fields on the System Information Page

Field	Description
Description	Type of system platform (for example, OS1052 or OS1063)
System Uptime	Amount of time since the last system reboot
Serial Number	Unique serial number assigned to the physical unit
Software Version	Current software version running on the system
System Name	The name that you assign to the system
Location	The physical location that you assign to the system
Support Contact	The e-mail address of the of the nearest support center or system engineer servicing the system

Click on **Refresh** to update all fields on the **System Information** page with the most recent information.

Note The **System Information** page also contains information about the **System Uptime** and **Software Version**. **System Uptime** indicates the time that has passed since the last system reboot. **Software Version** indicates the current software version running on the system.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

System Information

192.168.168.162 > System Information

System Description: S1063
System Uptime: 1h:20m:41s
Serial Number: 1063Z0611US00013
Software Version: Rel_4.2.0Build188
Power Supply Type: AC
System Name: Alpha 1
Location:
Support Contact:

Data Refreshed on - Thursday, May 17, 2007 6:35:44 PM

Figure 10. Configuring the System Identity

Ethernet LAN Management Port Settings

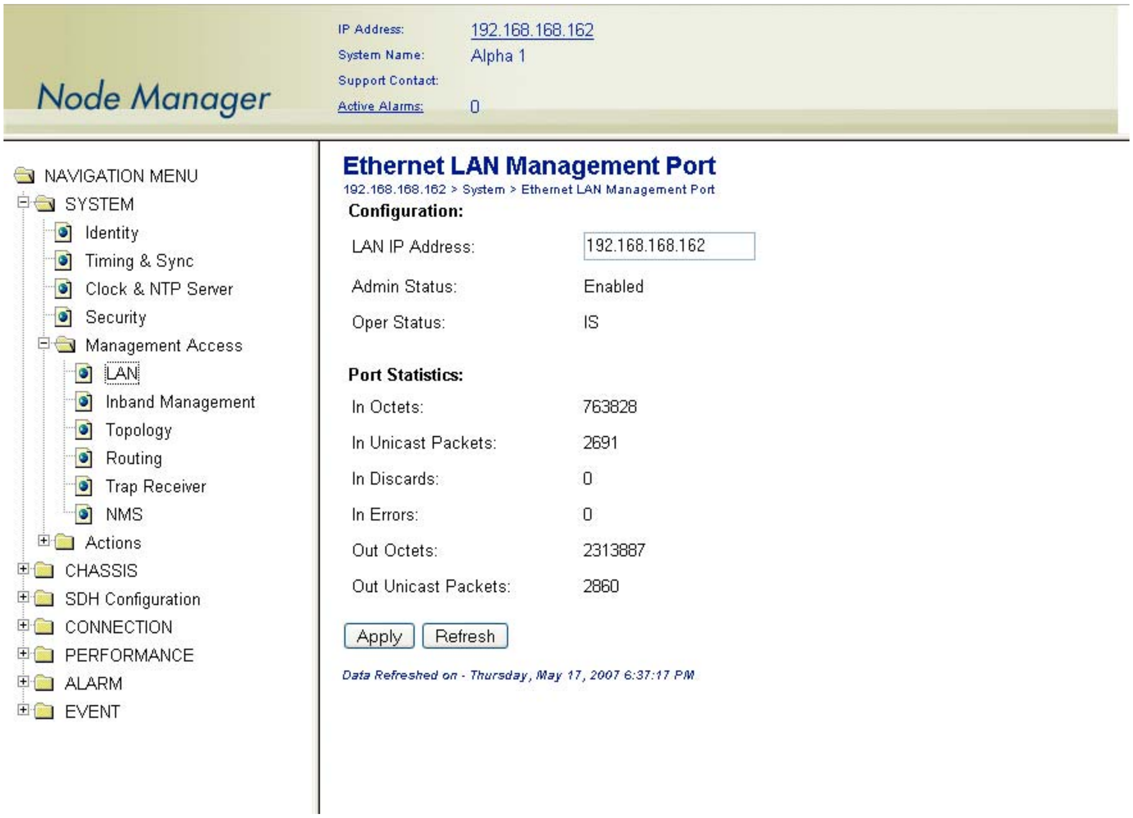
The following section provides the procedures for configuring the IP address and default gateway settings for the Ethernet LAN management port.

Configuring the Port Settings

To configure the Ethernet LAN management (LM) port settings, see Figure 18 and follow these steps:

> **Note** You may skip the following task if the IP address, net mask, and default gateway are already configured using the CLI, as indicated in §6.4.

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Management Access**.
3. From the expanded **Management Access** folder, select **LAN**.
4. On the **Ethernet LAN Management Port** page, type the required **IP Address**.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Ethernet LAN Management Port

192.168.168.162 > System > Ethernet LAN Management Port

Configuration:

LAN IP Address:	192.168.168.162
Admin Status:	Enabled
Oper Status:	IS

Port Statistics:

In Octets:	763828
In Unicast Packets:	2691
In Discards:	0
In Errors:	0
Out Octets:	2313887
Out Unicast Packets:	2860

Data Refreshed on - Thursday, May 17, 2007 6:37:17 PM

Figure 11. Configuring the Ethernet LAN Management Port

Changing the Default Gateway for the LAN Port

To change the default gateway for the Ethernet LAN management port, follow these steps:

Note Use this procedure to allow an NMS or a GUI client device to reach the system through the LAN port from a different IP subnet.

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Management Access**.
3. From the expanded **Management Access** folder, select **Routing**.
4. On the **Route Table** page, click on **Add Route**.
5. On the **Add New Route** page, select the **LM:** interface using the scroll-down button.

Note LM: is the interface notation for the Ethernet LAN port.

6. Type the new default gateway on the **Gateway** field, and leave the rest of the fields blank.

Note The new default gateway is the IP address of the router on the IP subnet to which the LAN port is connected. Through this router the system can access the IP subnet in which the NMS or GUI client device resides.

7. Click on **Apply** and then on **Close** to close the window.
8. Save the system configuration.

CAUTION

Save the system configuration to prevent the loss of the IP settings when a system reset or reboot occurs.

Inband Management Channel

The system uses inband management channels (IMC) for internal IP-based communications between network elements in an OnSite OS-10 Series subnetwork. The IMC also provides a path for reaching an OS-10 Series subnetwork from a centralized OnSight NMS or GUI client device.

Note A subnetwork consists of all interconnected nodes in a point-to-point, ring, or linear network. The subnetwork may contain a mix of OS-10 Series nodes, such as the OS1052 and OS1063.

The following sections describe two methods for setting up the IMC. The first method uses the data communications channel (DCC) bytes on the STM-1 signal. The second method uses an embedded E1 payload signal within a VC-12 container.

Each system has two IMC ports. The ports are designated using the following convention: IM:slot/port. IM:1/1 refers to the first inband management (IM) channel in slot 1. IMC:1/2 refers to the second IM channel in slot 1. Table 10 on page 40 provides a description of these ports.

Note The IM ports are not physical but logical ports.

Table 10. Inband Management Channels on the OS-10 Series System

Inband Management Channel (IMC)	IMC Supporting IP over . . .
IM:1/1	DCC or E1 mapped into a selected TU-12 channel
IM:1/2	DCC only

SDH Data Communications Channel (DCC)

The system provides the option of using the STM-1 DCC bytes for IP-based communications between OnSite OS-10 nodes in a point-to-point, ring, or linear subnetwork.

Each subnetwork has a gateway network element (GNE). All nodes in the subnetwork have IP connectivity and communicate with the OnSight NMS or GUI client device through the LAN port of the GNE.

By default, the system uses HDLC to encapsulate IP packets into the DCC bytes. The OSPF routing protocol is used to route IP packets within the subnet. The system supports an autodiscovery feature (embedded within the HDLC packets) to retrieve and display IP address information from adjacent nodes in a subnetwork.

Table 18 provides a list of the configurable options for the DCC bytes.

Table 11. DCC Properties

Property	Configurable Option
Admin Status	Enabled or Disabled
Type	DCCr, DCCm, or DCC custom

Note The DCCr option is the regenerator section DCC and uses the D1 to D3 bytes in the STM-1 section overhead as a 192-kbit/s channel between two systems.

Note The DCCm option is the multiplex section DCC and uses the D4 to D12 bytes in the STM-1 section overhead as a 576-kbit/s channel between two systems.

The DCC custom option allows the selection of any subset of DCC rows to form the DCC channel. You can form a custom DCC channel from four rows (see Table 12). Each row supports a 192-kbit/s channel. The system supports the creation of higher-rate DCC channels by combining two or more DCC rows into a single custom channel. For instance, you can create a custom DCC channel at 384-kbit/s by selecting any two DCC rows (for example, rows 1 and 2 or 2 and 3) or a full-rate DCC channel at 768-kbit/s by selecting all four DCC rows.

Table 12. DCC Byte Structure

Row	DCC Bytes
1	D1 to D3
2	D4 to D6
3	D7 to D9
4	D10 to D12

The system supports a DCC transparency feature that allows unselected rows to be transferred from one STM-1 port to another. For instance, if the first DCC row (DCCr) is selected for use by STM-1 ports 1 and 2 on the base system, the remaining DCC rows (2 to 4) are transferred transparently between the two ports. The system processes IP packets from only the selected DCC rows. All other rows are relayed without processing from one STM-1 port to the other.

Note DCC transparency works between STM-1 ports on the same slot, that is, between STM-1 ports 1 and 2 on the base system (slot 1) or between ports 1 and 2 on an STM-1 expansion module (in slot 2 or 3).

The DCC transparency feature is important for applications that require interworking between OnSite OS-10 Series platforms and third-party SDH network elements on the same SDH ring or linear network. For instance, an eight-node ring may consist of two third-party SDH nodes and six OnSite nodes. If the thirdparty SDH nodes are set to process the DCCr (row 1), the OnSite nodes would be set to process the remaining DCC rows (2 to 4). This setting allows the DCCr to pass through transparently between the STM-1 ports of the OnSite nodes.

Figure 12 shows sample usage of the DCC in a four-node OS-10 ring subnetwork. In this example, the host, NMS server, and GNE LAN port reside in the same IP subnet.

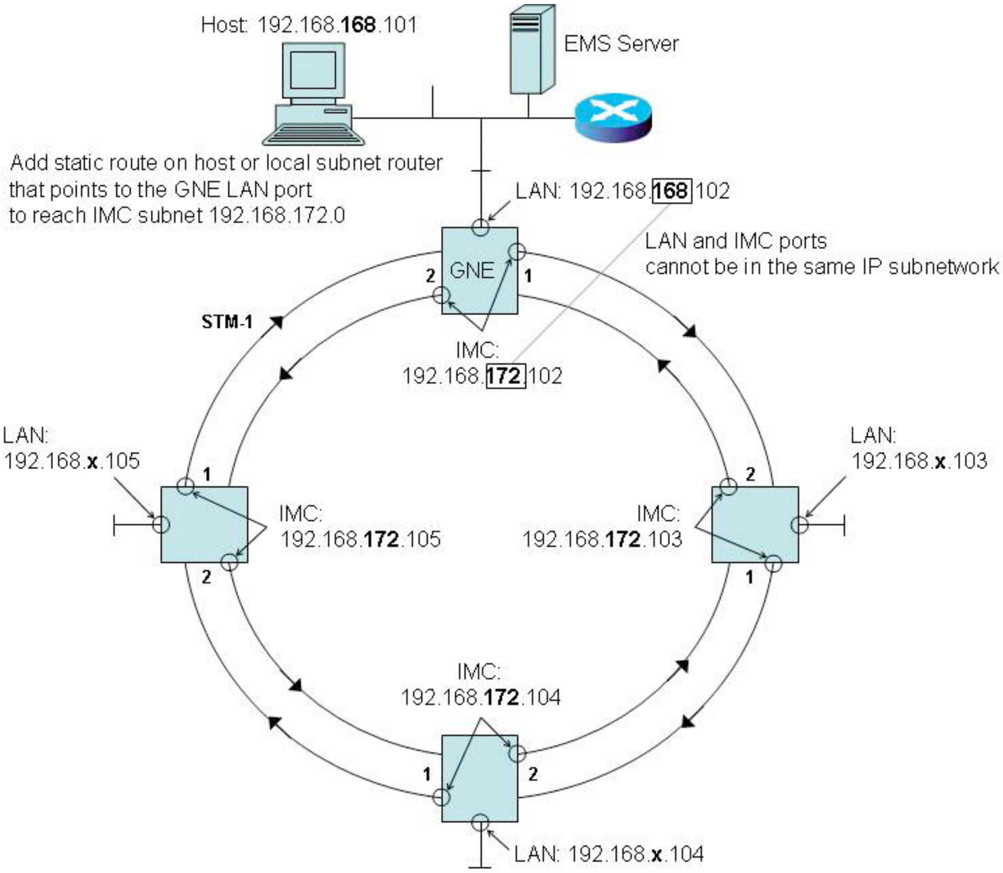


Figure 12. Example of IMC Using the SDH DCC in a Ring Subnetwork

Figure 13 shows sample usage of the DCC in a point-to-point subnetwork that uses Linear 1+1 MSP protection.

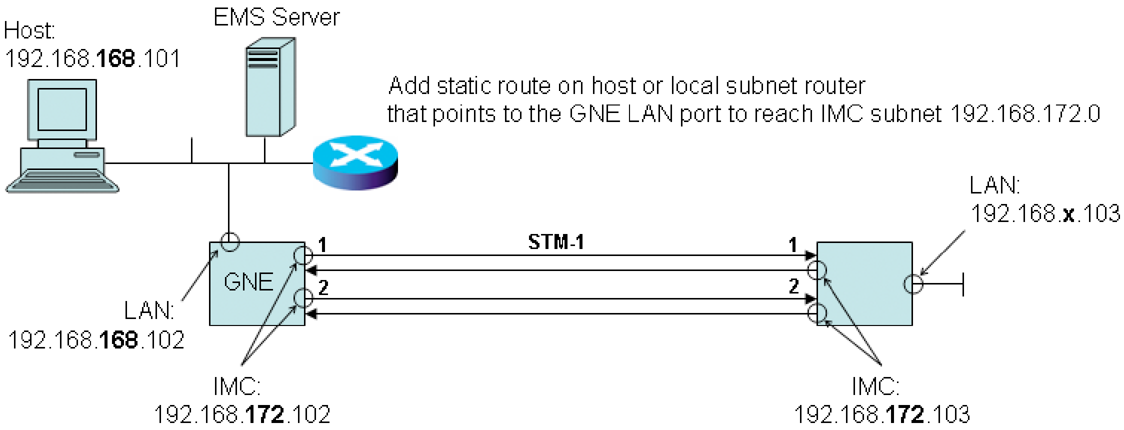


Figure 13. Example of IMC Using the SDH DCC in a Point-to-Point Subnetwork

To configure the IMC settings for the SDH DCC bytes, see Figure 21 and follow these steps:

Before starting the procedure, make sure that all STM-1 ports in the subnetwork are enabled (see §8.2.1) and that no alarms are present at the STM-1 RS and MS layers. In addition, make sure that the STM-1 ports of ADM nodes in a ring or linear network are connected according to the fiber interconnection procedures.

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Management Access**.
3. From the expanded **Management Access** folder, select **Inband Management**.
4. On the **Inband Management Channel** page, select **IM:1/1** and click on **Properties**.
5. In the **Inband Management Channel Properties** window, set the **Admin Status** to **Enabled**.

Note By default, the **Admin Status** for the IMC ports is set to **Disabled**.

6. Select the IMC **Type** (**DCCr**, **DCCm**, or **DCC custom**).

   – Select the **STM-1 Port** from which you wish to process the DCC channel, using the scroll-down list.

If you select **DCC custom**, follow Step 6B to select the rows of **DCC bytes** that form the custom DCC channel; otherwise, continue with Step 7.

   – Select the rows of DCC bytes from the DCC Bytes list.

The system highlights the first row of DCC Bytes (**D1 to D3**) by default. You may, however, choose other rows from the list.

To select more than one row from the list, click on individual list entries while pressing the Ctrl key. (The system highlights any entry that you select from the list. You can select any entry from the list, whether the rows are contiguous or not.)

7. Type the **IMC IP Address** for IM:1/1.

Note Use the **Reset** button to cancel any recent configuration changes in the window and revert to the settings before the window was opened. The reset works only before you commit the changes using the **Apply** button (see Step 8).

CAUTION Changing the IMC IP address settings for a node could result in the loss of management connectivity to the system if the connection is currently through the IMC port.

8. Click on **Apply** to apply the new IMC IP settings.
9. Click on **Close** to close the window.
10. Repeat steps 1 through 9 for the second IMC port (IM:1/2).

Note The IMC IP addresses for IM:1/1 and IM:1/2 need to be the same.

CAUTION Save the system configuration to prevent the loss of the IMC IP settings if a system reset or reboot occurs.

11. Repeat Step 1 through Step 10 for all nodes in the OS-10 subnetwork.

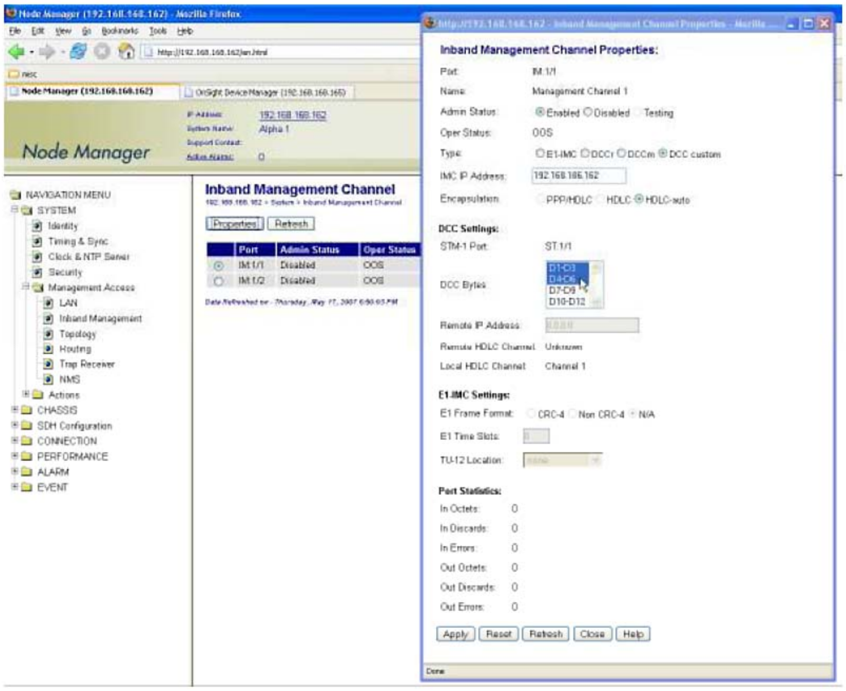
Note Make sure that all nodes use the same set of DCC bytes (DCCr, DCCm, or DCC custom).

- Make sure that all IMC ports are in the same IP subnet.
- Make sure that the LAN and IMC ports are not in the same IP subnet.

12. Verify that all DCC links in the OS-10 subnetwork are up.

Note The **Oper Status** of the IMC port should change from **OOS** to **IS** when the IMC ports that define the DCC link between two nodes are operational. This change may take a few seconds. Click on **Refresh** to update the window with the most recent contents. You may need to refresh the window more than once while you wait for the change to occur.

Note You may use the performance statistics for the IMC as an indicator of link activity and functional verification during the initial setup procedure. Click on **Refresh** to update the window with the most recent counts.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Inband Management Channel

192.168.168.162 > System > Inband Management Channel

	Port	Admin Status	Oper Status
●	IM 1/1	Disabled	OOS
○	IM 1/2	Disabled	OOS

Date Refreshed on - Thursday, May 17, 2007 6:50:03 PM

Inband Management Channel Properties:

Port: IM 1/1
Name: Management Channel 1
Admin Status: ● Enabled ○ Disabled ○ Testing
Oper Status: OOS
Type: ○ E1-IMC ○ DCCr ○ DCCm ● DCC custom
IMC IP Address: 192.168.186.162
Encapsulation: ○ PPP/HDLC ○ HDLC ● HDLC-auto

DCC Settings:

STM-1 Port: ST 1/1
DCC Bytes: D1-D3, D4-D6 (selected); D7-D9; D10-D12
Remote IP Address: 0.0.0.0
Remote HDLC Channel: Unknown
Local HDLC Channel: Channel 1

E1-IMC Settings:

E1 Frame Format: ○ CRC-4 ○ Non CRC-4 ● N/A
E1 Time Slots: 0
TU-12 Location: none

Port Statistics:

In Octets: 0
In Discards: 0
In Errors: 0
Out Octets: 0
Out Discards: 0
Out Errors: 0

Figure 14. Configuring the SDH DCC

Setting Up the IP Settings for Reaching the IMC Subnetwork

To allow the OnSight NMS or GUI client device to connect with any node in the IMC subnet, you must first set a static IP route on the host or local router (see Figure 12 on page 41 and Figure 13 on page 42). The static route must point to the GNE LAN port to reach the IMC subnet.

To allow communications for all hosts and servers, have your network administrator set up a static route on your local subnet router. Alternatively, you can set a route for an individual host or server.

If your NMS server or GUI client device is a PC that supports a DOS-based operating system, follow these steps to set up a static IP route between the PC and IMC subnet:

Note Follow these steps if no local router is present on the subnet on which the host resides and you prefer to connect the host directly to the GNE LAN port.

1. Open the Command Prompt window for your operating system and type the following command:

```
route add aaa.bbb.ccc.ddd mask eee.fff.ggg.hhhh iii.jjj.kkk.lll
```

Note The address aaa.bbb.ccc.ddd is the destination network. This address is the internal IP subnet for the IMC ports.

Note The net mask eee.fff.ggg.hhh is 255.255.255.0.

Note The address iii.jjj.kkk.lll is the gateway address and corresponds to the IP address of the GNE LAN management port.

For example, in Figure 12 on page 41, the required command to add a static route between the host and IMC subnet through the GNE LAN port would be:

```
route add 192.168.172.0 mask 255.255.255.0 192.168.168.102
```

2. Press Enter to apply the static route setting on your PC.

CAUTION

Make sure that you save the static route configuration permanently to avoid losing management connectivity to the subnetwork in case of a PC reboot.

Connecting to the Subnetwork

After the OnSight NMS or GUI client device is able to reach the GNE and the IMC is configured, you can begin managing the entire OS-10 subnetwork from your centralized location.

To initiate management connectivity from a GUI client device to any node in the subnetwork, type the IP address of the system in the Address field of the GUI client Web browser. This procedure opens the OnSight Device Manager for the selected system.

The OnSight NMS, however, provides full visibility of all nodes in the OnSite OS-10 subnetwork when the NMS has IP connectivity to the GNE.

E1 Inband Management Channel (E1-IMC)

The system provides the option of using an E1-based inband management channel (E1-IMC). The E1-IMC uses G.704 framing to carry IP packets on selected E1 time slots using PPP or HDLC encapsulation. You can assign any available TU-12 time slot on the STM-1 signal to carry the E1-IMC across an SDH network.

Table 13 lists the configurable options for the E1-IMC signal.

Table 13. E1-IMC Properties

Property	Configurable Options
Admin Status	Enabled or Disabled
Frame format	CRC-4 or non-CRC-4
Number of time slots	Time slots 1 through 31 (contiguous)
Packet data encapsulation	PPP over HDLC, HDLC, or HDLC-auto

Figure 15 on page 46 shows an application for the E1-IMC in which two OnSite OS-10 nodes are connected in a point-to- point configuration. The OnSight NMS reaches the remote node through a local node that serves as the gateway network element (GNE) for the point-to-point subnetwork. The GNE encapsulates IP packets from the LAN port into the E1-IMC and uses a selected VC-12 channel for connectivity across the STM-1 link.

Note For this configuration, you may choose to use the DCC bytes instead of the E1-IMC.

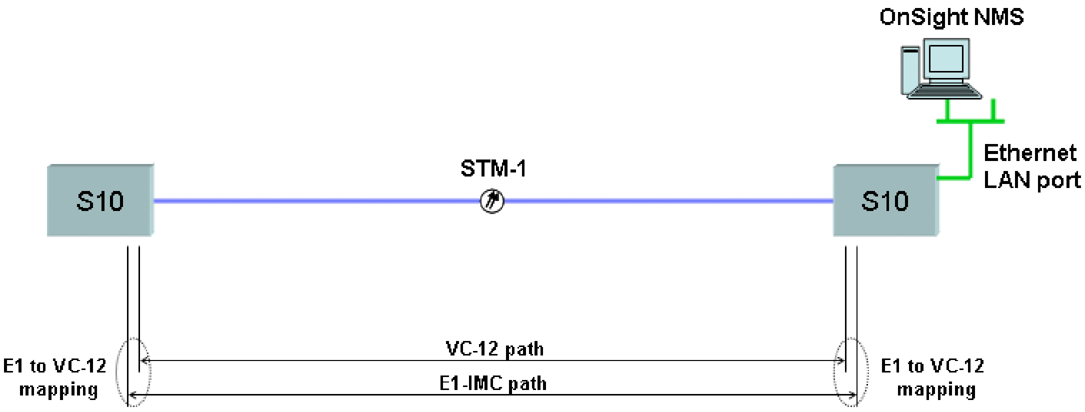


Figure 15. E1-IMC Application 1: Direct Point-to-Point

Figure 16 shows another application for the E1-IMC in which two OnSite OS-10 nodes are connected in a point-to-point configuration across a third-party SDH network. The OnSight NMS reaches the remote node through the GNE. The GNE encapsulates IP packets from the LAN port into the E1-IMC and uses a selected VC-12 channel to connect the IMC transparently across the SDH cloud.

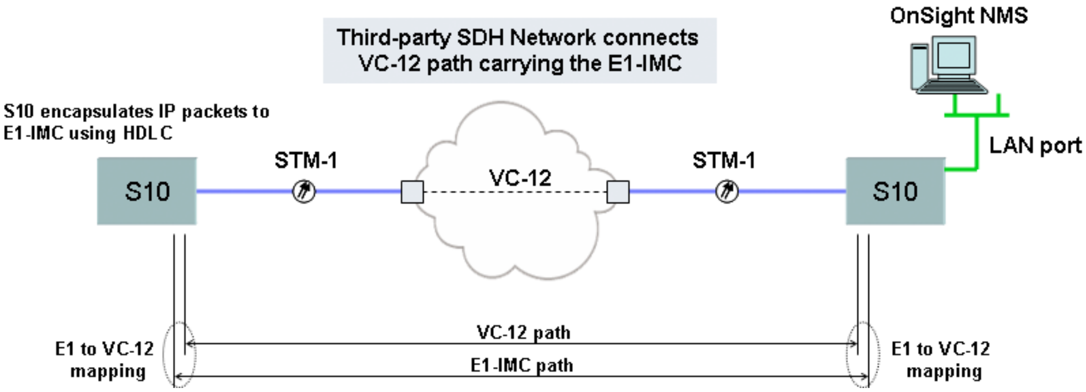

Third-party SDH Network connects VC-12 path carrying the E1-IMC
OnSight NMS
S10 encapsulates IP packets to E1-IMC using HDLC
STM-1
VC-12
STM-1
LAN port
S10
S10
E1 to VC-12 mapping
VC-12 path
E1-IMC path
E1 to VC-12 mapping

Figure 16. E1-IMC Application 2: Point-to-Point Across SDH Network

Configuring the E1-IMC Settings

To configure the E1-based IMC settings, see Figure 24 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Management Access**.
3. From the expanded **Management Access** folder, select **Inband Management**.
4. On the **Inband Management Channel** page, select **IM:1/1** and click on **Properties**.

Note Only IM:1/1 can be set for operation as an E1-IMC.

5. In the **Inband Management Channel Properties** window, set **Admin Status** to **Enabled**.

Note By default, the Admin Status for the IMC ports is set to Disabled.

6. Set the **IMC Type** to **E1-IMC**.
7. Type the **IMC IP Address** for the E1-IMC port.

CAUTION Changing the IP address, net mask, and default gateway settings for the IMC could result in the loss-of-management connectivity to the system, if the connection is currently through the IMC port.

8. Select the **E1 Frame Format** (**CRC-4** or **non-CRC-4**)

Note By default, the system uses the CRC-4 framing format. Time slot 0 is set according to the selected G.704 E1 frame format (whether CRC-4 or non-CRC-4). Make sure that frame format is the same on both sides of the E1-IMC link.

9. Type the **E1 Time Slots** (**1 to 31**).

Note By default, the system uses E1 time slots 1 through 31 for carrying payload data. You may use a reduced number of time slots for carrying payload data; however, make sure that the time slot setting is the same on both sides of the E1-IMC link.

10. Select the **Encapsulation** method (**PPP/HDLC**, **HDLC**, or **HDLC-auto**).

Note PPP/HDLC means PPP over HDLC.

Note Use HDLC (Auto) when connecting two OS-10 systems directly in a point-to-point configuration. This encapsulation method enables autodiscovery and retrieval of the IP address for the remote system.

11. If you do not use HDLC-auto as the encapsulation method, type the **Remote IP Address** for the E1-IMC on the adjacent OS-10 node.

Note The system fills this address field automatically when the encapsulation method is set to HDLC (Auto).

12. Select the TU-12 time slot location of the VC-12 that carries the E1-IMC signal, using the **TU-12 Location** scroll-down button.

Note The scroll-down list displays only the TU-12 time slot locations that remain available.

Note Make sure that the GNE and remote node use the same TU-12 time slot location for the E1-IMC.

13. Click on **Apply** to apply the new IMC IP settings.

CAUTION

Save the system configuration to prevent the loss of the IMC IP settings if a system reset or reboot occurs.

14. Click on **Close** to close the window.

15. Repeat Step 1 through Step 13 for both nodes.

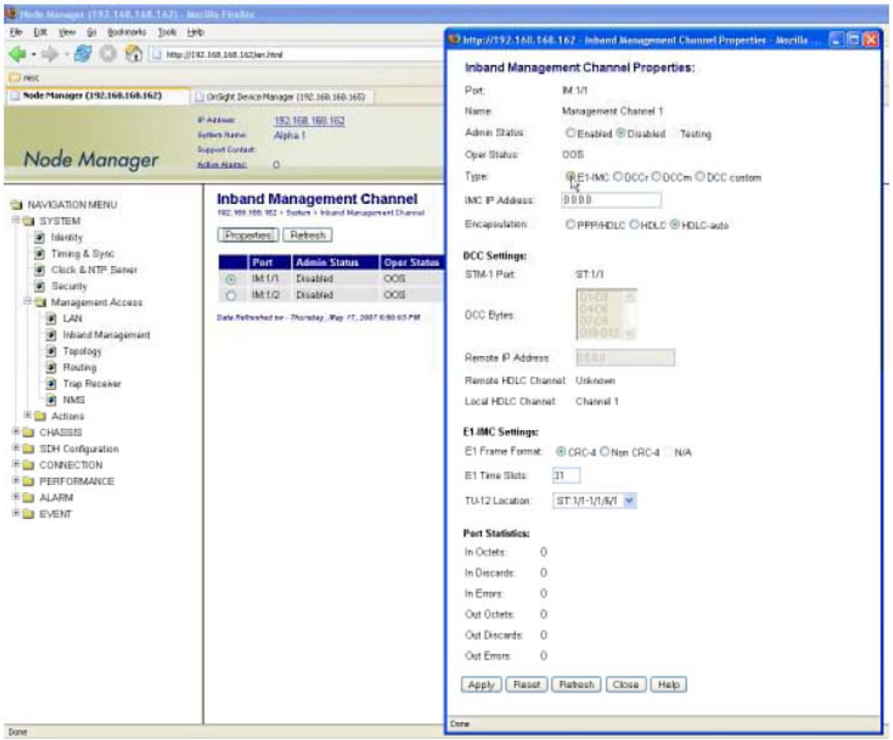
Note Make sure that both nodes use the same frame format, time slots, and encapsulation.

- Make sure that the IMC ports on both nodes are in the same IP subnet.
- Make sure that the LAN and IMC ports are not in the same IP subnet.

16. Verify that the E1-IMC link between the two nodes is up.

Note The **Oper Status** of the IMC port should change from **OOS** to **IS** when the IMC ports that define the E1-IMC link between two nodes are operational. This change may take a few seconds. Click on **Refresh** to update the window with the most recent contents. You may need to refresh the window more than once while you wait for the change to occur.

Note You may use the performance statistics for the IMC as an indicator of link activity and functional verification during the initial setup procedure. Click on **Refresh** to update the window with the most recent counts.


Node Manager (192.168.168.162) - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.168.162/an.html
Node Manager (192.168.168.162)
OnSight Device Manager (192.168.168.165)
Node Manager
NAVIGATION MENU
SYSTEM
Identity
Timing & Sync
Clock & NTP Server
Security
Management Access
LAN
Inband Management
Topology
Routing
Trap Receiver
NMS
Actions
CHASSIS
SDH Configuration
CONNECTION
PERFORMANCE
ALARM
EVENT
Properties
Refresh
Done
http://192.168.168.162 - Inband Management Channel Properties - Mozilla ...
Apply
Reset
Refresh
Close
Help
Done

IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Inband Management Channel

192.168.168.162 > System > Inband Management Channel

	Port	Admin Status	Oper Status
●	IM:1/1	Disabled	OOS
○	IM:1/2	Disabled	OOS

Date Refreshed on - Thursday, May 17, 2007 6:50:03 PM

Inband Management Channel Properties:

Port: IM:1/1
Name: Management Channel 1
Admin Status: ○ Enabled ● Disabled ○ Testing
Oper Status: OOS
Type: ● E1-IMC ○ DCCr ○ DCCm ○ DCC custom
IMC IP Address: 0.0.0.0
Encapsulation: ○ PPP/HDLC ○ HDLC ● HDLC-auto

DCC Settings:

STM-1 Port: ST:1/1
DCC Bytes: D1-D3 D4-D6 D7-D9 D10-D12
Remote IP Address: 0.0.0.0
Remote HDLC Channel: Unknown
Local HDLC Channel: Channel 1

E1-IMC Settings:

E1 Frame Format: ● CRC-4 ○ Non CRC-4 ○ N/A
E1 Time Slots: 31
TU-12 Location: ST:1/1-1/1/6/1

Port Statistics:

In Octets: 0
In Discards: 0
In Errors: 0
Out Octets: 0
Out Discards: 0
Out Errors: 0

Figure 17. Configuring the E1 Inband Management Channel

Configuring a Default Gateway for the E1-IMC

If you do not use HDLC (Auto) as the encapsulation method, you must also set the default gateway route for the E1-IMC port on the remote OS-10 node. The new default gateway for this port should be set to the IP address of the E1-IMC port on the GNE.

To change the default gateway for the E1-IMC port on the remote node, follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Management Access**.
3. From the expanded **Management Access** folder, select **Routing**.
4. On the **Route Table** page, click on **Add Route**.
5. On the **Add New Route** page, select the **IM:1/1** interface using the scroll-down button.
6. Type the new default gateway on the Gateway field, and leave the rest of the fields blank.

Note The new default gateway is the IP address of the E1-IMC port on the GNE.

Note For example, in Figure 25, the required settings for changing the default gateway for theE1-IMC on the remote node would be as follows: Destination is 0.0.0.0, Mask is 0.0.0.0, and Gateway is 192.168.172.102.

7. Click on Apply and then on Close to close the window.
8. Save the system configuration.

CAUTION

Save the system configuration to prevent the loss of the IP settings if a system reset or reboot occurs.

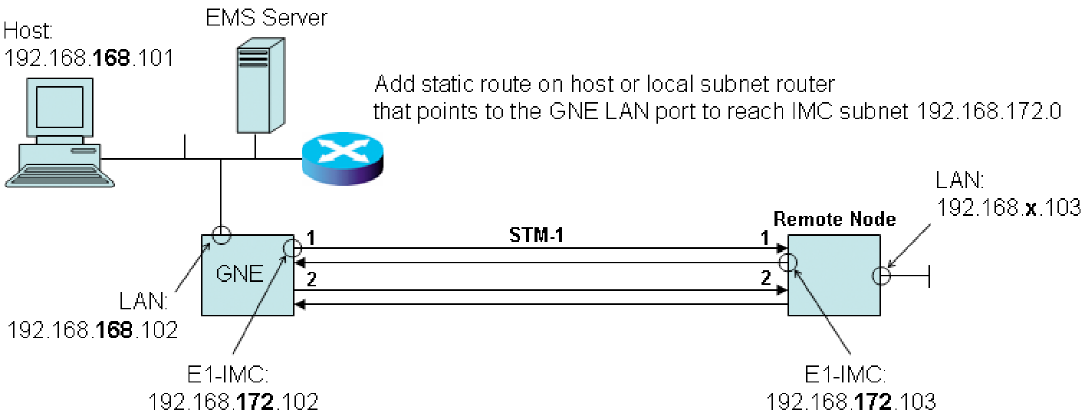


Figure 18. Example of Using the E1-IMC in a Point-to-Point Subnetwork

Monitoring the E1-IMC Alarms and Performance

The system monitors the following E1 path defects associated with the E1-IMC:

- AIS (alarm indication signal)
- LFA (loss of frame alignment), according to G.706
- RDI (remote defect indicator using the A bit), according to G.704

To display E1-IMC alarms, if present, follow these steps:

1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Show Active Alarms**.

At this point, the **Active Alarms** page displays all active alarms in the system, including E1-IMC alarms, if present. The table contains a separate entry for each active E1-IMC alarm. Table 14 describes the fields for each E1-IMC alarm entry.

Table 14. Table Entries for Active E1-IMC Alarms

Table Entry for Active Alarms	Field Value
Type	**E1 AIS, E1 LFA,** or **E1 RDI**
Alarm Raised Time	Date and time
Severity	Critical, Major, Minor, or Warning
Detailed Information	Location of affected inband management channel (IM:1/1)

Note The system automatically updates the **Active Alarm**s page every 60 seconds. Click on **Refresh** if you need to update the table with the most recent active alarm information. Individual table entries automatically clear whenever previously active alarms are no longer present.

The system calculates the following E1 path error performance events, as listed in Table 15, for the E1-IMC in accordance with Recommendations G.826 and G.829:

Table 15. E1 Path Error Performance Events for the E1-IMC

PM Parameter	Description	Definition
BBE	Background Block Error	An EB (errored block) not part of an SES
ES	Errored Second	A second containing at least one EB or a defect (LFA or AIS)
SES	Severely Errored Second	A second containing K or more EBs or a defect (LFA or AIS)
UAS	Unavailable Second	A period of unavailable time that begins at the onset of 10 consecutive SES

Note A period of unavailable time begins at the onset of 10 consecutive SES seconds. These 10 seconds are part of unavailable time. A period of available time begins at the onset of 10 consecutive non-SES seconds. These 10 seconds are part of available time.

To display current and historical PM data for the E1-IMC, follow these steps:

1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select **Counters**.
3. From the expanded **Counters** folder, select **Inband Management**.

At this point, the **Inband E1 Near-end PM – Current 15 minutes** page shows the near-end PM data for the current 15-minute period only.

Note The PM data is not updated automatically as new events occur during the Current 15-minute and 24-hour periods. Click on **Refresh** to update the tables with the most recent cumulative count for the current periods.

Continue with the step that follows to display historical PM data for both 15-minute and 24-hour periods.

4. Select the table entry for the **IM:1/1** port and click on **Show Interval**.

Note The tables display **Invalid** under **PM data** when the data collected during a measurement period is considered invalid. **Interval Start Time** also displays n/a (not available).

Timing and Synchronization

The system supports two timing modes: Internal and Auto. Table 16 describes these modes.

Table 16. System Timing Modes

Timing Mode	Description
Internal	The system is synchronized to the internal oscillator. This mode is also known as forced free-run.
Auto	The system is synchronized using one or two timing reference sources. These sources are designated as the primary and secondary sources.

Note The default timing mode at power up is Internal,

Note The internal system clock is of Stratum 3 (± 4.6 ppm) quality.

To display the type of clock installed in your system, follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Slots**.
3. Select the table entry for Slot ID number 1 (the base system) and click on **Properties**.

The **Stratum Type** field indicates the stratum quality of the system clock (Stratum 3).

Auto Mode Operation

In Auto mode, the system remains in the initial free-run state until a valid timing source becomes available on either the primary or secondary reference source. You can select the primary and secondary sources from several reference input candidates. Table 17 summarizes the available sources.

Table 17. Timing References for Synchronization in Auto Mode

Reference	Primary	Secondary	Timing Mode	Timing Source
Pair 1	STM-1 port 1	STM-1 port 2	Line timing	Derived clock from STM-1 line
Pair 2	E1 port 7 (OS1052) E1 port 20 (OS1063)	E1 port 8 (OS1052) E1 port 21 (OS1063)	Line timing	Derived clock from E1 line when both E1 ports are configured to carry traffic
			External timing	Incoming 2.048-MHz clock when both E1 ports are configured as Sync In

Note If the OS1052 is equipped with T1 interfaces on the base system, the second reference pair is T1 port 7 and port 8. For an OS1063 with T1 interfaces on the base system, the second reference pair is T1 ports 20 and 21. The system uses the incoming 1.544-MHz clock when these T1 ports are configured as Sync In.

Note If the system is equipped with HD-E1 expansion modules, the system presents additional timing reference pair options using E1 ports 20 and 21 on those modules.

If both timing references are available, the system uses the primary reference as the active source and the secondary as the standby source.

In Auto mode, the system can be in one of three states, as listed in Table 18:

Table 18. Timing States

Timing State	Description
Free-run	This state is the initial state until a valid timing reference becomes available.
Normal	The system is locked to either the primary or secondary reference.
Holdover	The system was previously in the Normal state, and both the primary and secondary references are unavailable. This state also occurs if the primary reference is unavailable, the secondary reference is available, and either a “Lockout” or “Forced to Primary” external command is present. The system reverts from the Holdover to the Normal state when either the primary or secondary reference becomes available.

If the primary reference fails, the system automatically switches to the secondary reference in a hitless manner. The switchover does not occur if either a “Lockout” or a “Forced to Primary” external command is present. The system considers an input timing reference as unavailable according to the criteria in Table 19.

Table 19. Criteria for Declaring an Input Timing Reference as Unavailable

Internal Clock	Input Timing Reference Is Unavailable when the . . .
Stratum 3 option	STM-1 signal is in LOS, LOF, or MS-AIS condition; or the incoming SSM code is DNU or invalid; or the E1 signal is in LOS condition
	Frequency is off by ± 12 ppm from nominal

The system reports an alarm condition when the primary or secondary reference fails.

Note In Holdover state, the Stratum 3 clock has the following characteristics: ± 0.37 ppm for the first 24 hours.

To configure the system timing mode, see Figure 19 on page 55 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Timing & Sync**.
3. On the **Timing & Synchronization** page, select one of the **Timing Mode – Primary/Secondary Source** options using the scroll-down button.

Note By default, **Timing Mode – Primary/Secondary Source** is set to **Internal**. In this mode, the system uses the local internal oscillator as the sole source of timing.

Choose **Auto: STM-1 port 1/1, port 1/2** for operation in Auto mode, using the derived clock from STM-1 ports 1 and 2 as the primary and secondary references, respectively.

Note If the system is configured for operation with a single unprotected STM-1 port, the system can still operate in Auto mode but with one of the two references always unavailable.

Choose **Auto: STM-1 port 1/1** only for operation in Auto mode, using the derived clock from STM-1 port 1 as the only timing source for the system. With this setting, the system goes inmmediately into holdover mode when STM-1 port 1 becomes unavailable as a timing reference.

Note This timing mode must be used for proper operation of OS-10 nodes in a 2-fiber (unprotected) linear ADM topology. All subtending OS-10 nodes in a linear ADM chain must be synchronized to the Master/Headend node using this timing source selection. Also, all subtending nodes in the chain must be configured with the Synchronization Status Messages (SSM) set to Disabled (see Figure 19 on page 55).

Note The linear ADM chain must start from STM-1 port 1/2 on the Headend node. This port should be connected to STM-1 port 1/1 of the first subtending OS-10 node in the chain and port 1/2 of this node should be connected to port 1/1 of the next node in the chain. All nodes in the chain must be connected to each other in like manner.

Choose **Auto: E1 port 1/7, port 1/8** in the OS1052 (or **Auto: E1 port 1/20, port 1/21** in the OS1063) for operation in Auto mode using the derived clock from E1 ports 7 and 8 in the OS1052 (or E1 ports 20 and 21 in the OS1063) as the primary and secondary references, respectively.

Note If only one E1 port is configured as Sync In, the system can still operate in Auto mode but with one of the two references always unavailable.

4. Click on **Apply** for the settings to take effect.

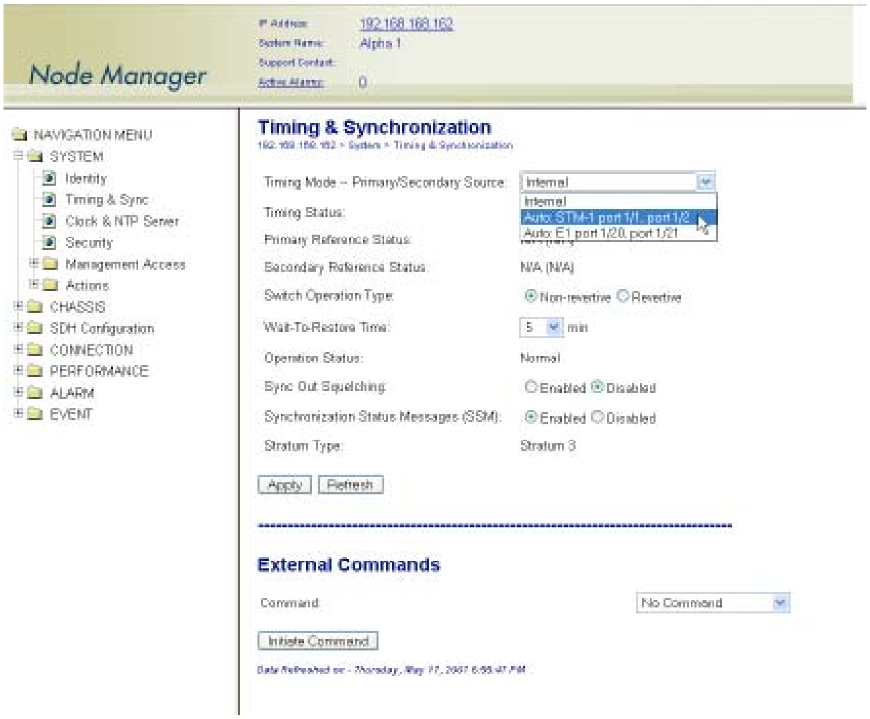
When Auto mode is selected, **Timing Status** on the **Timing & Synchronization** page changes from **Free-run** to **Normal** if the system is able to lock to one of the two timing references. Later, if no reference is available, **Timing Status** changes to **Holdover**.

Check **Primary Reference Status** and **Secondary Reference Status** to see the current status for each of the timing references. If the reference is available, the status indicator shows whether the reference is active or standby. For example, if the primary reference is available and the system is locked to this reference, the status indicator for this reference shows “active.” If the secondary reference is also available, the status indicator shows “standby” for this reference. The status indicator also shows the incoming synchronization status message (SSM) code for available references if the use of SSM codes is enabled.

Operation Status on the **Timing & Synchronization** page indicates **Normal** when both the primary and secondary references are available, with one reference active and the other in standby mode. **Operation Status** indicates **Unavailable reference** when one or both references are unavailable and either a “Lockout” or “Forced to Primary” external command is present.

Click on **Refresh** to update the page with the most current status information.

NOTE: The system does not allow changing the timing mode directly from **Auto: STM-1 port 1/1, port 1/2** to **Auto: E1 port 1/7, port 1/8** in the OS1052 (or **Auto: E1 port 1/20, E1 port 1/21** in the OS1063). You must first change the timing mode to Internal and then to **Auto: E1 port 1/7, port 1/8** (or **Auto: E1 port 1/20, port 1/21**).



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Timing & Synchronization

192.168.168.162 > System > Timing & Synchronization

Timing Mode – Primary/Secondary Source: Internal (Internal / Auto: STM-1 port 1/1, port 1/2 / Auto: E1 port 1/20, port 1/21)

Timing Status:

Primary Reference Status:

Secondary Reference Status: N/A (N/A)

Switch Operation Type: ● Non-revertive ○ Revertive

Wait-To-Restore Time: 5 min

Operation Status: Normal

Sync Out Squelching: ○ Enabled ● Disabled

Synchronization Status Messages (SSM): ● Enabled ○ Disabled

Stratum Type: Stratum 3

External Commands

Command: No Command

Data Refreshed on - Thursday, May 17, 2007 6:55:47 PM

Figure 19. Configuring the System Timing Mode

The system supports two types of switch operation for timing references: revertive and non-revertive. Table 20 describes these operations.

Table 20. Switch Operation Types for Timing

Operation Type	The System . . .
Revertive	Switches back to the primary reference after the primary reference becomes available. The system waits for a preset amount of time (that is, the wait-to-restore time) before the switchover from the secondary to the primary reference occurs.
Non-revertive	Stays locked to the secondary reference even after the primary reference becomes available. A switchover back to the primary reference either occurs after completion of an external switch command (forced or manual) or after recovery of the primary reference and subsequent failure of the secondary reference.

To configure the switch operation type, see figure 19 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Timing & Sync**.
3. On the **Timing & Synchronization** page, select one of the **Switch Operation Type options: Non-revertive or Revertive.**

Note By default, Switch Operation Type is set to Non-revertive.

To change the wait-to-restore time, continue with Step 4; otherwise, go directly to Step 5 to complete this task.

Note The wait-to-restore time is applicable only when using revertive switching. Its value is ignored when using non-revertive switching.

4. On the **Timing & Synchronization** page, change **Wait-To-Restore Time** from the factory default setting of 5 (minutes) to any integer value between **0 and 12** minutes.
5. Click on **Apply** for the settings to take effect.

When revertive mode is selected, **Operation Status** on the **Timing & Synchronization** page indicates **Wait-to-Restore** (**WTR**) after a timing reference switchover has occurred and the system is waiting to switch back to the primary reference after completion of the WTR time.

External Commands for Timing Reference Switching

The system allows the use of external commands to switch between the Primary and Secondary references. Table 21 lists the external commands that the system supports:

Table 21. External Commands for Timing Reference Switching

Priority	Command	Action	Completion
1	Clear	Clears all switch commands	Always
2	Lockout	Disables a switch to the secondary reference	Always
3	Forced to Secondary	Switches from the primary to the secondary reference	Denied if the invalid signal condition is present on the secondary reference or if the Lockout command is present
	Forced to Primary	Switches from the secondary to the primary reference	Denied if the Lockout command is present
4[a]	Manual to Secondary	Switches from the primary to the secondary reference	Denied if the invalid signal condition is present on the secondary reference or if the Lockout or Forced command is present
	Manual to Primary	Switches from the secondary to the primary reference	Denied if the invalid signal condition is present on the primary reference or if the Lockout or Forced command is present

[a] Manual switching is hitless.

To activate any of the external commands for timing reference switching, see Figure 20 on page 57 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Timing & Sync**.

3. On the **Timing & Synchronization** page, select one of the **Command** options in Table 21 on page 56.

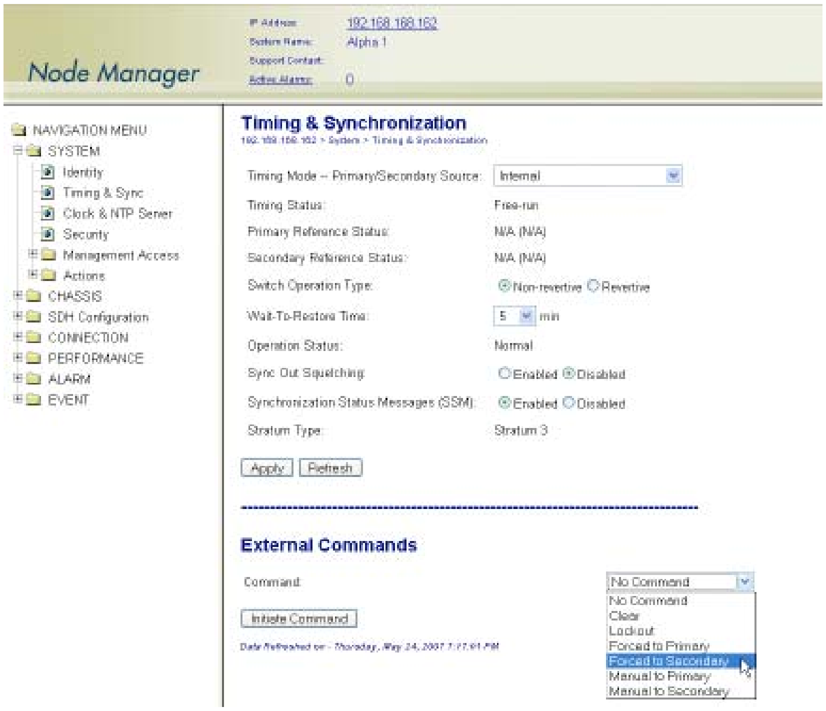
> **Note** By default, Command is set to No Command.

4. Click on **Initiate Command** to activate the external command.

> **Note** Use external commands only when system operation is in Auto timing mode.

5. To reset any active command, select the **Clear** command option and click on **Initiate Command**. Otherwise, the current command remains active until a higher priority command is issued or a failure event occurs (see Table 21).

Operation Status on the **Timing & Synchronization** page indicates **Manual**, **Forced**, or **Lockout** when an external command is active.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Timing & Synchronization

192.168.168.162 > System > Timing & Synchronization

Timing Mode -- Primary/Secondary Source: Internal
Timing Status: Free-run
Primary Reference Status: N/A (N/A)
Secondary Reference Status: N/A (N/A)
Switch Operation Type: ● Non-revertive ○ Revertive
Wait-To-Restore Time: 5 min
Operation Status: Normal
Sync Out Squelching: ○ Enabled ● Disabled
Synchronization Status Messages (SSM): ● Enabled ○ Disabled
Stratum Type: Stratum 3

External Commands

Command: No Command

Date Refreshed on - Thursday, May 24, 2007 7:17:01 PM

Figure 20. Configuring the External Commands for Switching Timing References

S1-Byte Support

The system generates and uses the synchronization status message (SSM) codes and quality levels for "Option I SDH synchronization networking" in G.781, as shown in Table 22.

Table 22. SSM Codes and Quality Levels Supported on the OS-10

Quality Level	SSM COde (S1 Bits 5-8)
PRC	0010
SSU-A	0100
SSU-B	1000
SEC	1011
DNU	1111

Note The system uses the code for SSU-B for Stratum 3 systems in free-run mode.

The system rejects an incoming STM-1 port as a timing reference source (that is, the system considers the reference as unavailable) if the incoming SSM for the port has the DNU code.

To enable the use of the SSM, see Figure 26 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Timing & Sync**.
3. On the **Timing & Synchronization** page, set **Synchronization Status Messages** (SSM) to **Enabled**.
4. Click on **Apply** to complete this task.

Note The **Timing & Synchronization** page (see Figure 19 on page 55) shows the Sync Quality Level for the primary and secondary timing reference sources. The system translates the incoming SSM code into the equivalent Sync Quality Level for the source.

External Synchronization

You can configure E1 ports 7 and 8 in the base OS1052 system (or E1 ports 20 and 21 in the base OS1063 system) individually in one of three modes:

- Traffic
- Synchronization input (Sync In)
- Synchronization output (Sync Out)

By default, the system uses E1 ports 7 and 8 in the base OS1052 system (or E1 ports 20 and 21 in the base OS1063 system) for carrying regular E1 traffic. When the ports carry E1 traffic and the timing mode is set to **Auto: E1 port 1/7, port 1/8** in the OS1052 (or **Auto: E1 port 1/20, port 1/21** in the OS1063), the system uses the derived clock from these ports as the primary and secondary references for the system.

When these ports are configured in Sync In mode and the timing mode is set to **Auto**, the system uses external timing input signals at 2.048 MHz as the primary and secondary references for the system. The external timing inputs do no carry traffic and comply with the physical layer specifications in G.703 for external 2.048-MHz synchronization signals.

Note In Sync Out mode, the E1 port requires the use of an external 3dB attenuator to bring the voltage level for the 2.048 MHz synchronization signal down to the required level in G.703.

When the system is synchronized to external timing inputs using the Sync In ports, the system generates the SSM codes (see Table 29) in accordance to the quality level that you assign to these ports. The quality level should be set in accordance to the quality of the timing source that generates the 2.048-MHz signals. For example, if the system receives timing from an SSU-A (or BITS) clock through the E1 Sync In ports, you should set the quality level of the E1 Sync In ports to SSU-A.

When either E1 port 7 or E1 port 8 in the OS1052 (or E1 port 20 or port 21 in the OS1063) is configured in Sync Out mode, the system generates a G.703-compliant synchronization signal at 2.048 MHz. With this setting, it is not possible to set the timing mode to Auto using these ports.

Sync Out Squelching

The system provides the option of squelching the Sync Out ports. The squelching function turns off the transmitter of the Sync Out ports when the timing mode changes to Internal or the system enters into the Free-run state. The system removes the squelching when locked again to either the primary or secondary reference.

Clock and NTP Server

The system supports the ability to obtain real-time clock (RTC) information from a network time protocol (NTP) server. The clock information is used for time-stamping when required.

The system also allows manual configuration of the clock whenever access to an NTP server is not possible.

To configure the system date and time with an NTP server, see Figure 21 on page 60 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Clock & NTP Server**.
3. On the **System Clock** page, set **NTP Services** to **Enabled**.

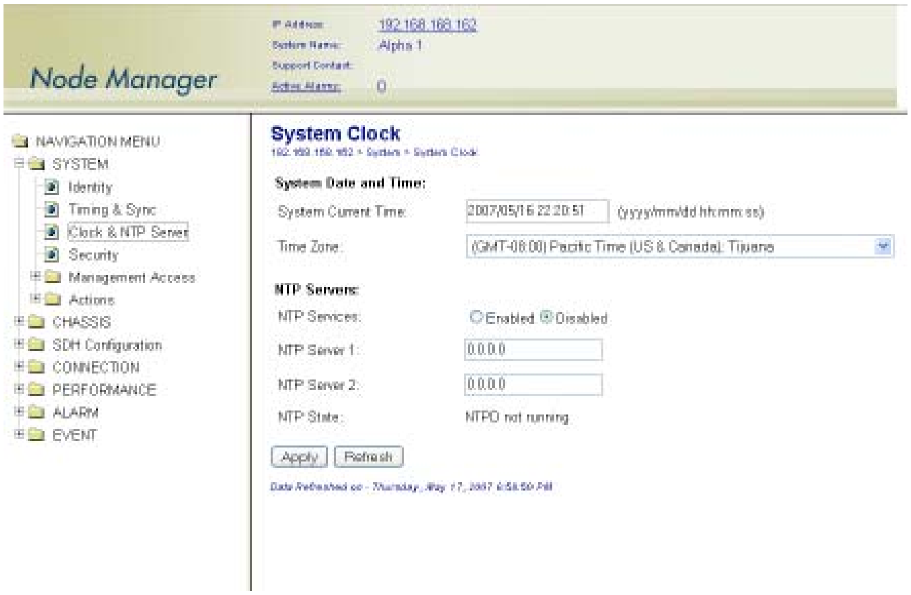
Note By default, **NTP Services** is set to **Disabled**.

4. Type the IP address for **NTP Server 1** and for **NTP Server 2**, if required.
5. Click on **Apply** to initiate connectivity to the NTP servers.

At this point, **NTP State** changes to **NTPD running** when the system finds and updates the system clock using one of the NTP servers.

Click on **Refresh** to retrieve the most current **NTP State** and **System Current Time**.

Note The system maintains the date and time settings for up to 8 hours after power is removed from the system.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

System Clock

192.168.168.162 > System > System Clock

System Date and Time:

System Current Time: 2007/05/16 22:20:51 (yyyy/mm/dd hh:mm:ss)

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

NTP Servers:

NTP Services: ○ Enabled ● Disabled

NTP Server 1: 0.0.0.0

NTP Server 2: 0.0.0.0

NTP State: NTPD not running

Data Refreshed on - Thursday, May 17, 2007 6:58:50 PM

Figure 21. Configuring Access to an NTP Server

To configure the system clock manually, follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Clock & NTP Server**.
3. On the **System Clock** page, set **NTP Services** to **Disabled**.
4. To modify the local time zone, use the **Time Zon**e scroll-down button to select the new time zone and click on **Apply.** Go directly to Step 7 if the current setting for the time zone is correct.

> **Note** The factory default for the time zone is GMT (Greenwich Meridian Time, also known as Coordinated Universal Time). The system automatically adjusts the current time according to the daylight saving time requirements for your time zone, when needed.

5. Save the system configuration to prevent the loss of the new time zone setting when the system reboots.
6. Reboot the system to apply the new time zone settings. (After completion of the reboot, repeat Step 1 and Step 2, and continue with Step 7).
7. Type the **System Current Time** in the specified format (yyyy/mm/dd hh:mm:ss).

> **Note** The time format includes the year (yyyy), month (mm) and day (dd), and the hour (hh), minutes (mm) and seconds (ss). The hour is in 24-hour format.

8. Click on **Apply** to put the new current time into effect.

Security

The system supports three types of users, as shown in Table 23:

Table 23. User Types and Privileges

User Type	This User Type Permits . . .
Super	Read and write operations on all items. The Super user can set up and manage IP addresses, user accounts, and passwords. Only one Super user can exist.
Admin	Read and write operations on most items. The Admin user cannot set up user accounts, and passwords.
Monitor	Read-only operations.

Note The factory-assigned default password for the Super user is super (all lowercase letters). The Super user can change his or her and can also reset the password of Admin and Monitor users to the factory-assigned default. The Super user can also change the Admin or Monitor user password to any valid alphanumeric string if required.

- The factory-assigned default password for an Admin user is admin (all lowercase letters). An Admin user cannot change his or her password.
- The factory-assigned default password for a Monitor user is monitor (all lowercase letters). A Monitor user cannot change his or her password.
- For all user types, the password must be 5 to 12 characters in length, and can contain only the following alphanumeric characters: lower case letters (a through z), upper case letters (A through Z), numbers (0 through 9), hyphens (-), commas (,), colons (:),underscores (_), slashes (/), periods (.), spaces, parentheses, and the @ character.

WARNING

If the Super user wishes to access the system but forgets his or her password, it is necessary to restore the system to the factory default settings.

To change the user password, follow these steps:

Note The following procedure only applies to the Super user. The system denies this operation for Admin and Monitor users.

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Security**.
3. From the expanded **Security** folder, select **Manage User**.

4. On the **User Management** page, select the user for which you wish to change the password and click on **Change Password**.
5. In the **Change Password** window, type the **New Password**, and **Confirm Password** fields.
6. Click on **Apply** for the new password to be in effect and then on **Close** to close the window.

Note For Admin and Monitor users, contact the Super user if you forget the password.

To reset a password back to factory default, follow these steps:

Note The following procedure only applies to the Super user. The system denies this operation for Admin and Monitor users.

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Security**.
3. From the expanded **Security** folder, select **Manage User**.
4. On the **User Management** page, select the user for which you wish to reset the password and click on **Reset Password to Default**.

System Actions

This section includes procedures for the downloading and upgrading of the system software. It also includes procedures for initiating a system reset and saving the current system configuration. The section ends with procedures for restoring the system to the factory default configuration and instructions for transferring the system configuration and log files to and from a server.

Downloading System Software

The system allows the downloading and installation of new software images from local or remote locations using FTP or TFTP. The OS-10 system flash memory contains two partitions for the software image: Active and Standby. Table 24 describes each memory partition.

Table 24. Software Image Memory Partitions

Memory Partition	Contains the . . .
Active	Current software image. The system uses this image to boot and run its operating system and applications.
Standby	Standby software image. This image may differ from the image in the Active partition. The software downloading process places the new Standby software image. This image may differ from the image in the Active partition. The software downloading process places the new

To download and install software into the Standby memory partition, see Figure 22 on page 64 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select the **Actions** folder.

3. From the expanded **Actions** folder, select **Download Software**.
4. On the **Download and Install Software Image for Upgrade** page, set **Transfer Protocol** to **FTP** or **TFTP**.

Note FTP is the default transfer protocol. FTP and TFTP work on Windows, UNIX, and Linux servers.

5. Type the **Host Pathname** to indicate the name of the software image file to be retrieved and its location within the host server.

Note You must specify either the full pathname or the relative pathname from the server root directory to indicate the location of the software image file. The file name for the software image must contain the .img extension.

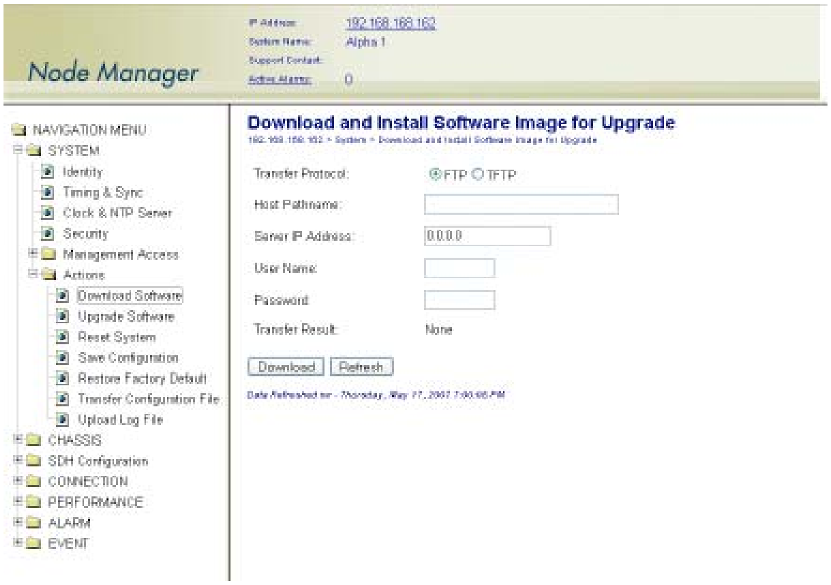
6. Type the **Server IP Address** of the host server containing the software image file.
7. Type the **User Name** and **Password** for secure access to the file.

Note In this step, you must enter the user name and password, as demanded by the server access permission.

8. Click on **Download** to initiate the file transfer between the server and OS-10 system.

Note The software downloading process takes a few minutes to complete. The system continues normal operation while the downloading process takes place.

- A progress window indicates the percentage of completion. Click on **Cancel** to terminate the file transfer process at any time.
- The interruption of the file transfer process causes corruption of the software image in the Standby partition. The system does not allow the selection of the Standby image for system bootup if the file is corrupted.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Download and Install Software Image for Upgrade

192.168.168.162 > System > Download and Install Software Image for Upgrade

Transfer Protocol: ● FTP ○ TFTP

Host Pathname:

Server IP Address: 0.0.0.0

User Name:

Password:

Transfer Result: None

Date Refreshed on - Thursday, May 17, 2007 7:00:00 PM

Figure 22. Downloading and Installing the System Software

Upgrading System Software

To upgrade the system software from the current image in the Active memory partition to the image in the Standby memory partition, see Figure 23 on page 65 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select the **Actions** folder.
3. From the expanded **Actions** folder, select **Upgrade Software**.
4. On the **Software Image Upgrade** page, select **Image Source for Next Reboot** using the scrolldown button.

> **Note** The system displays **No image installed (standby)** if no image is present in the Standby partition.

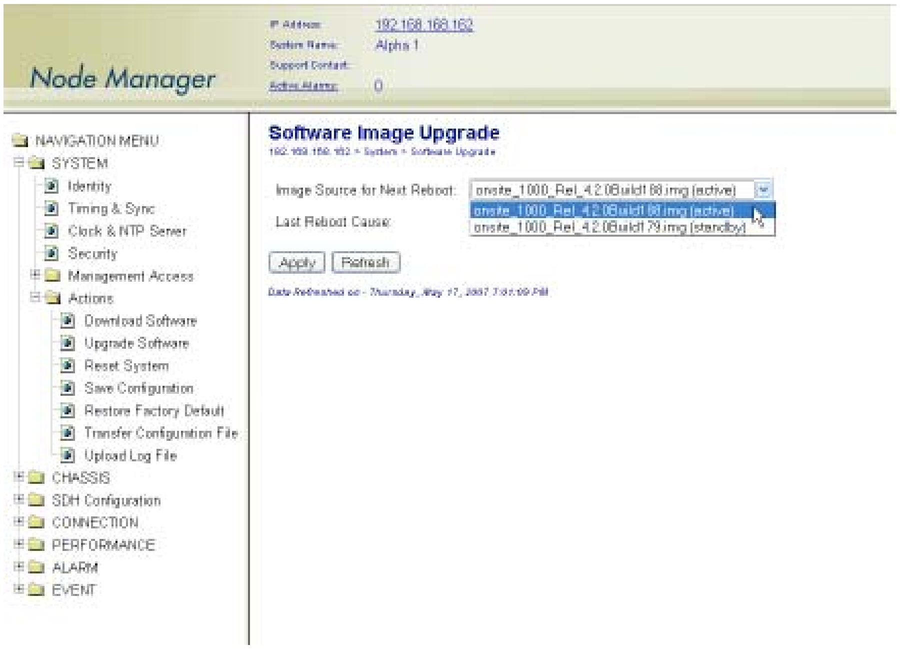
5. Click on **Apply** to confirm the selection of the new image and begin the system reboot process.

At this point, the system begins the reboot process using the software image in the **Image Source for Next Reboot** field.

> CAUTION
>
> This action initiates a cold reboot if the new image contains firmware changes; otherwise, the system begins a warm reboot process. A warm reboot does not result in traffic interruption while the reboot process takes place. Consult your software release notes to see if installation of the new image results in either a warm or cold reboot.

WARNING

A cold reboot results in traffic interruption while the reboot process takes place. Make sure that you first save the system configuration to the flash memory to prevent the loss of configuration data. The system uses the last saved configuration to restore system operation and traffic connectivity after the completion of the reboot. Any recent configuration data and connections not saved to the system configuration file are lost and need reentry, if required.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Software Image Upgrade

192.168.168.162 > System > Software Upgrade

Image Source for Next Reboot: onsite_1000_Rel_4.2.0Build168.img (active)

onsite_1000_Rel_4.2.0Build168.img (active)
onsite_1000_Rel_4.2.0Build179.img (standby)

Last Reboot Cause:

Data Refreshed on - Thursday, May 17, 2007 7:01:09 PM

Figure 23. Upgrading the System Software

Resetting the System

The system supports two types of reset: warm reset and cold reset. To reset the system using the Webbased management interface, follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select the **Actions** folder.
3. From the expanded **Actions** folder, select **Reset System**.
4. On the **System Reset** page, click on **Warm Reset** to reset the system using a warm reboot. Alternatively, to reset the system using a cold reboot, click on **Cold Reset**.

A warning window opens to alert you to the start of the system reset process using a warm or cold reboot. Click on **OK** to continue or **Cancel** to cancel the request.

Note A warm reboot does not result in traffic interruption while the reboot process takes place.

⚠ WARNING **A cold reboot results in traffic interruption while the reboot process takes place. Make sure that you first save the system configuration to the flash memory to prevent the loss of configuration data. The system uses the last saved configuration to restore system operation and traffic connectivity after the completion of the reboot. Any recent configuration data and connections not saved to the system configuration file are lost and need reentry, if required.**

Note Another way to cause the system to reset and reboot is to initiate a power cycle. A power cycle occurs when you turn off the system and then turn it back on. For systems using AC power, use the on-off switch on the rear panel. For systems using DC power, use the on-off switch on the circuit breaker or rectifier unit that supplies power to the system.

⚠ CAUTION After turning off the AC power switch, wait for at least 3 seconds before turning it back to the on position.

⚠ WARNING **Do not touch the DC power contacts on the front panel when power is applied to the system.**

Saving the System Configuration

To save the system configuration to the flash memory, follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select the **Actions** folder.
3. From the expanded **Actions** folder, select **Save Configuration**.
4. On the **Save Configuration** page, click on **Save Configuration**.

A warning window opens to alert you to the start of the save-configuration process. Click on **OK** to continue or **Cancel** to cancel the request.

WARNING

This action causes the system to overwrite the current configuration data stored in the flash memory. The system uses the last saved configuration to restore system operation and traffic connectivity after the completion of a reboot. Any recent configuration data and connections not saved to the system configuration file are lost and need re-entry, if required.

Restoring the Factory Default Settings

To restore the factory default settings for the system, follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select the **Actions** folder.
3. From the expanded **Actions** folder, select **Restore Factory Default**.
4. On the **Reset Configuration to Factory Default** page, click on **Reset Configuration to Factory Default**.

A warning window opens to alert you to the start of the restore-factory-default process. Click on **OK** to continue or **Cancel** to cancel the request.

WARNING

This action causes the system to overwrite the current configuration data stored in the flash memory with the original factory default settings and causes the system to perform a cold reboot. This reboot causes the permanent deletion of all current connections and custom configuration options. In addition, you may lose management connectivity to the system when the IP addresses of the management ports revert to factory default.

Transferring the System Configuration File

To transfer the system configuration file between an FTP/TFTP server and the system, see Figure 24 on page 69 and follow these steps:

Note The system configuration file is a binary file and is not user readable. When you upload the configuration file to a host server, the file is tied to the serial number of the system. The system does not allow the downloading of a configuration file that does not match the serial number of the system.

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select the **Actions** folder.
3. From the expanded **Actions** folder, select **Transfer Configuration File**.
4. On the **Transfer Configuration File** page, set the **Transfer Protocol** to **FTP** or **TFTP**.

Note FTP is the default transfer protocol. FTP and TFTP work on Windows, UNIX, and Linux servers.

5. Set **Transfer Action** to **Download** or **Upload**.

Note Use Upload if you wish to transfer the configuration file on the OS-10 to the FTP/TFTP server. Use Dowload, however, to transfer the file in the opposite direction – from the server to the OS-10.

6. Type the **Host Pathname** to indicate the name that you will give to the OS-10 configuration file and the location of this file within the host computer where the FTP/TFTP server resides.

Note You must specify either the full pathname or the pathname relative to the FTP/TFTP server root directory to indicate the location of the configuration file. When uploading the configuration file, the configuration file that resides on the OS-10 will be transferred and placed in the specified **Host Pathname** location. In the opposite direction – when downloading the configuration file into the OS-10, the configuration file that resides on the OS-10 will be replaced with the configuration file on the **Host Pathname** location.

Note The configuration file must not contain spaces. You can use hyphen (-) or undercore (_) instead of spaces. The configuration file name need not have any extension but it is recommended that you use the .cfg extension for ease of reference. It is also recommended that that the file name includes information such as the system name and the date the configuration file was last saved.

7. Type the **Server IP Address** of the host computer on which the FTP/TFTP server resides.

8. Type the **User Name** and **Password** for secure access to the file. In this step, you must enter the user name and password, as demanded by the FTP server access permission. (If you use TFTP, the user name and password are not required and should be left empty.)

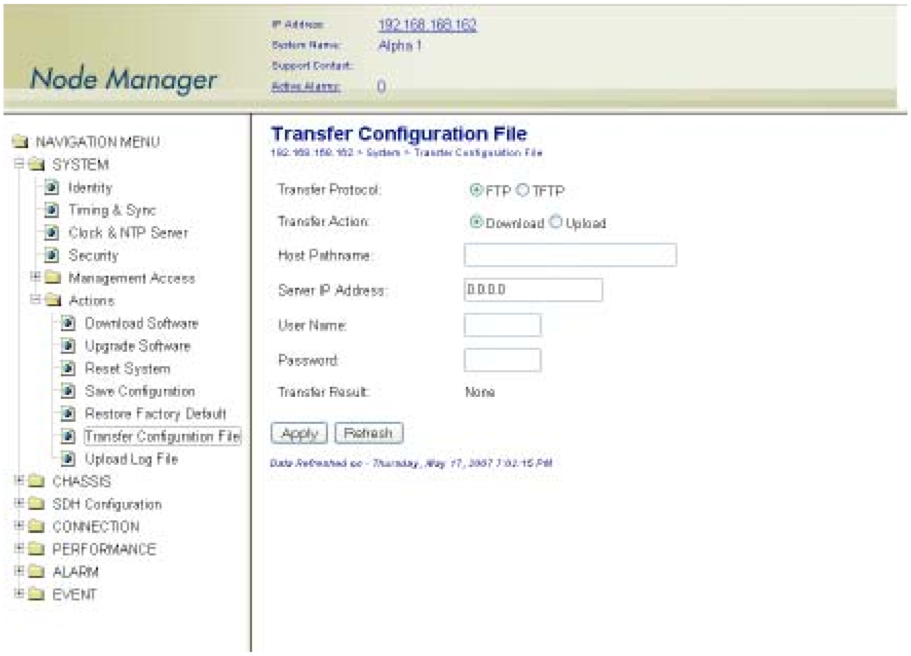
9. Click on **Apply** to initiate the file transfer between the server and OS-10 system.

Note The file transfer process may take from a few seconds to one or two minutes to complete, depending on the size of the file. The system continues normal operation while the downloading process takes place.

- A progress window indicates the percentage of completion. Click on **Cancel** to terminate the file transfer process at any moment.

- **Transfer Result** on the **Transfer Configuration File** page indicates the status of the file transfer; that is, whether the transfer is still in progress or has been completed.

- The interruption of a download-file-transfer process causes corruption of the configuration file.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Transfer Configuration File

192.168.168.162 > System > Transfer Configuration File

Transfer Protocol: ● FTP ○ TFTP
Transfer Action: ● Download ○ Upload
Host Pathname:
Server IP Address: 0.0.0.0
User Name:
Password:
Transfer Result: None

Data Refreshed on - Thursday, May 17, 2007 7:02:15 PM

Figure 24. Transferring the System Configuration File

Uploading the System Log File

The system log file contains historical information on system-related activities. This file is for diagnostic purposes only.

> **Note** The system log file is an ASCII file and is user readable. The log file, however, is intended for use by system engineers or trained personnel servicing the OS-10 system.

To upload the system log file into a host server, see Figure 25 on page 71 and follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select the **Actions** folder.
3. From the expanded **Actions** folder, select **Upload Log File.**
4. On the **Upload Log File** page, set **Transfer Protocol** to **FTP** or **TFTP**.

> **Note** FTP is the default transfer protocol. FTP and TFTP work on Windows, UNIX, and Linux servers.

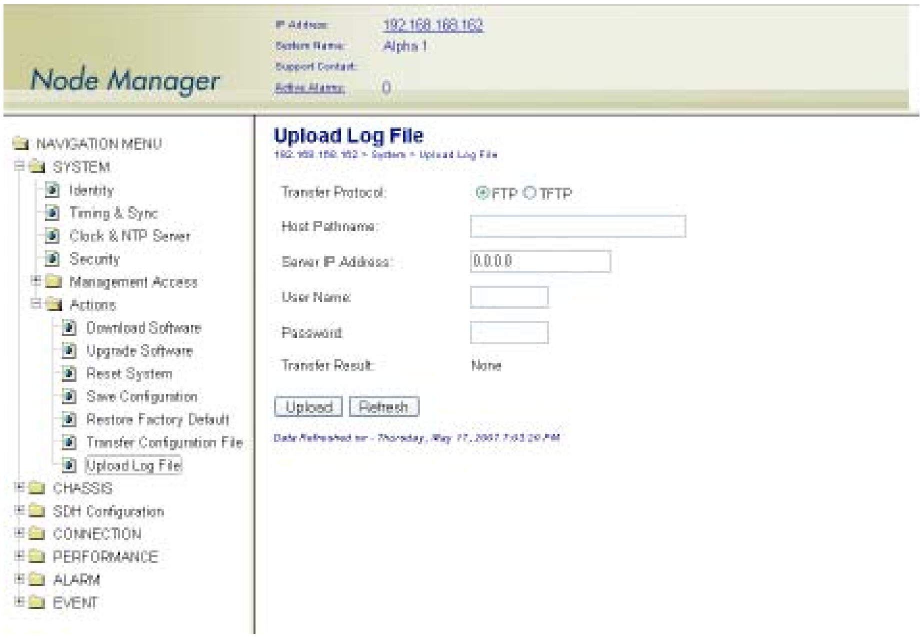
5. Type the **Host Pathname** to indicate the name of the system log file and its target directory within the host server.

> **Note** You must specify either the full pathname or the pathname relative to the server root directory to indicate the location of the log file. The log file name need not have any extension but it is recommended that you use the .log extension for ease of reference. It is also recommended that that the file name includes information such as the system name and the date the log file was last retrieved.

6. Type the **Server IP Address** of the host server.
7. Type the **User Name** and **Password** for secure access to the file. In this step, you must enter the user name and password, as demanded by the FTP server access permission. (If you use TFTP, the user name and password are not required and should be left empty.)
8. Click on **Upload** to initiate the file transfer between the server and OS-10 system.

> **Note** The log upload process may take from a few seconds to one or two minutes to complete, depending on the size of the file. The system continues normal operation while the upload process takes place.
>
> - A progress window indicates the percentage of completion. Click on **Cancel** to terminate the file transfer process at any time.
> - **Transfer Result** on the **Transfer Configuration File** page indicates the status of the file transfer; that is, whether the transfer is still in progress or has been completed.

- The interruption of the file transfer process causes corruption of the log file.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Upload Log File

192.168.168.162 > System > Upload Log File

Transfer Protocol: ● FTP ○ TFTP

Host Pathname:

Server IP Address: 0.0.0.0

User Name:

Password:

Transfer Result: None

Data Refreshed on - Thursday, May 17, 2007 7:03:20 PM

Figure 25. Uploading the System Log File

Chapter 3 STM-1 Interface

Chapter contents

Introduction

This chapter provides the procedures for provisioning, monitoring and testing of SDH STM-1 ports and VC-12, VC-3 and VC-4 termination points (TPs).

General Information

The base OnSite OS-10 system provides two (2) optical STM-1 ports for connection to the SDH network. The ports operate at 155.520 Mbit/s and can be configured to operate as dual unprotected ports or as a protected pair using Linear 1+1 MSP. The ports can also be configured in add-drop multiplexer (ADM) mode for operation in a ring network using SNCP path protection switching.

Note The factory default for the protection mode is unprotected.

The STM-1 supports the AU-4 payload structure and provides connectivity at the VC-4, VC-3, VC-12, and VC-11 levels, as shown in Figure 26.

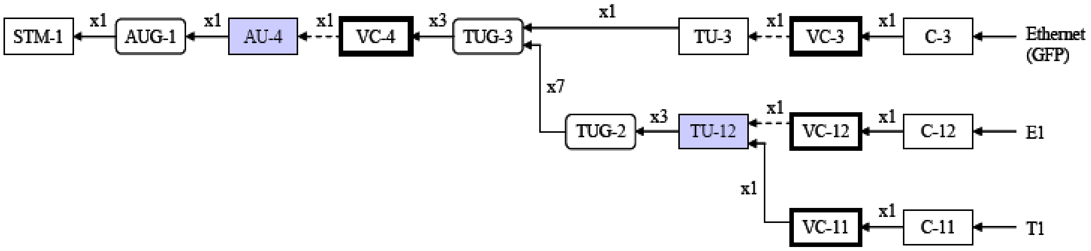


Figure 26. STM-1 AU-4 Multiplexing Structure

The STM-1 interface complies with the following standards:

- ITU-T G.707
- ITU-T G.783
- ITU-T G.826/G.829 (performance monitoring)
- ITU-T G.823 and G.783 (jitter and wander)
- ITU-T G.957 (optical parameters)

Figure 27 on page 75 shows the location of the STM-1 ports on the base OS1052 and OS1063 systems. The transmit (Tx) and receive (Rx) sides for each port are clearly labeled in the front panel.

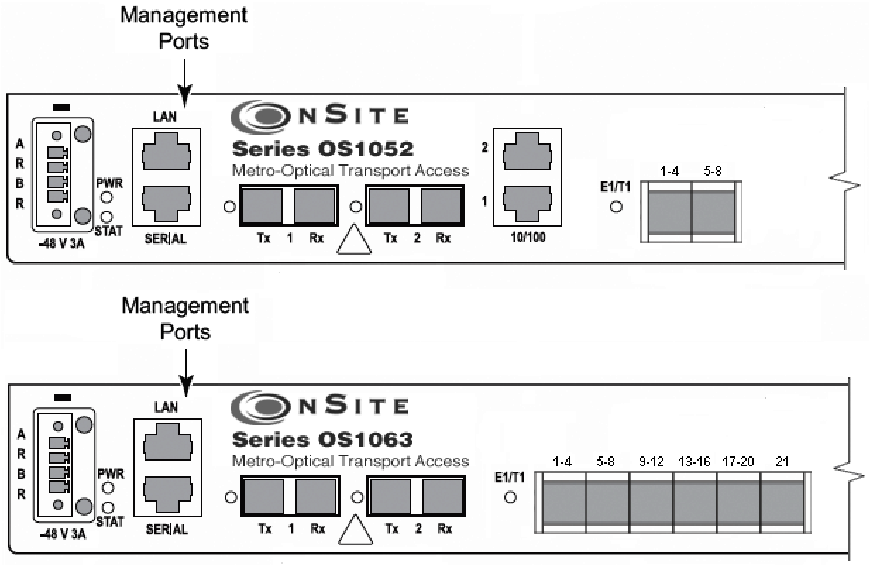


Figure 27. STM-1 Ports on the Base OS1052 and OS1063 Systems

Table 25 provides the interconnection parameters for the STM-1 ports.

Table 25. STM-1 Interconnection Parameters

Parameter	Type	Notes
Fiber Type	SMF (single mode fiber)	Standard G.652 fiber
Connector	SC	Duplex
Optical Reach	S-1.1	15 km at 1310 nm (G.957)
	L-1.1	15 km at 1310 nm (G.957)
	L-1.2	94 km at 1550 nm (G.957)

Table 26 summarizes the optical parameters for the S-1.1, L-1.1 and L-1.2 interfaces.

Table 26. Summary of S-1.1, L-1.1 and L-1.2 Optical Interface Parameters

Parameter		Unit	S-1.1	L-1.1	L-1.2
Wavelength	Operating range	nm	1261-1360	1263-1360	1480 to 1580
Mean launched power	Maximum	dBm	-8	0	0
	Minimum	dBm	-15	-5	-5
Attenuation	Range	dB	0 to 12	10 to 28	10 to 28
Receiver	Overload	dBm	-8	-10	-10
	Sensitivity	dBm	-23	-34	-34

Note The S-1.1, L-1.1 and L-1.2 optical interfaces are factory-installed options.

Note As a factory-installed option, the OS1063 platform is available with two STM-1 electrical interface (STM-1e) ports on the base system. The STM-1e ports comply with the G.703 specifications for electrical intefaces at 155.520 Mbit/s and use DIN 1.0/2.3 connectors for coaxial cables with 75-ohm impedance.

The maximum distances in Table 25 on page 75 for the S-1.1, L-1.1 and L-1.2 options are calculated based on the worst-case design approach in Annex A, G.957. Here, the maximum attenuation coefficient for installed G.652 fiber cable is specified as 0.8-dB/km for S-1.1, 0.5-dB/km for L-1.1, and 0.3-dB/km for L-1.2 applications. This coefficient includes the losses due to installation splices, repair splices and the operating temperature range. The actual maximum fiber interconnection distance is typically better than the worst-case design figure in G.957 and depends on the actual attenuation coeffiecient for the installed fiber plant (which is usually lower than the specified values in G.957). Also, the receiver sensitivity for the S-1.1, L-1.1 and L-1.2 interfaces on the OS-10 system is typically better than the values in G.957 by 3 dBm. Increased receiver sensitity results in a fiber span which is longer than the worst-case design value in G.957.

Note Use a power meter to ensure that the power level from the fiber that connects to the receive side of the STM-1 port is within the limits in Table 33 for the S-1.1, L-1.1 or L-1.2 interface whichever is used). You may need to use optical attenuators on the receive side of the port to prevent receiver overload when using short fiber cable lengths.

CAUTION To protect your eyes, never look at the transmit LED or laser through a magnifying device while it is powered on. Never look directly at a fiber port on the chassis or at the ends of fiber cable when they are powered on.

SDH Provisioning

The following section provides the procedures for enabling and disabling STM-1 ports. It also provides the procedures for configuring the STM-1 payload structure and the interface protection options.

Enabling an STM-1 Port

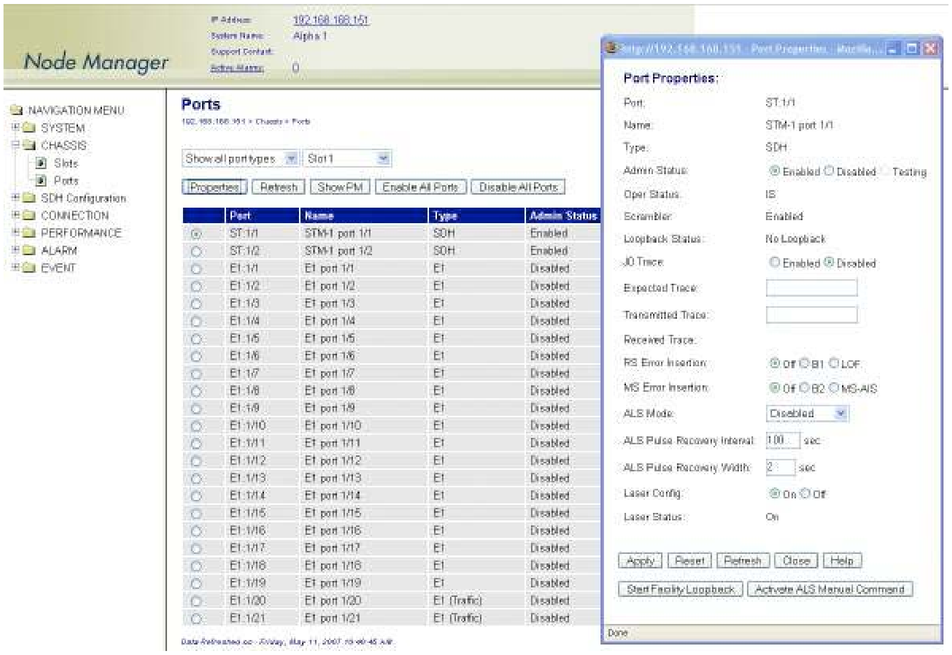
To configure an STM-1 port for service, see Figure 28 on page 77 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the STM-1 port being configured and click on **Properties**.

Note The system uses the following naming convention for STM-1 interfaces: ST:slot/port. The OS-10 contains two STM-1 ports in slot 1 (the base system), that is, ST:1/1 and ST:1/2.

4. In the **Port Properties** window, set **Admin Status** to **Enabled**.
5. Click on **Apply** and then on **Close** to close the window.

On the **Ports** page, **Admin Status** for the selected STM-1 port should now read **Enabled**.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Ports

192.168.168.151 > Chassis > Ports

	Port	Name	Type	Admin Status
●	ST:1/1	STM-1 port 1/1	SDH	Enabled
○	ST:1/2	STM-1 port 1/2	SDH	Enabled
○	E1:1/1	E1 port 1/1	E1	Disabled
○	E1:1/2	E1 port 1/2	E1	Disabled
○	E1:1/3	E1 port 1/3	E1	Disabled
○	E1:1/4	E1 port 1/4	E1	Disabled
○	E1:1/5	E1 port 1/5	E1	Disabled
○	E1:1/6	E1 port 1/6	E1	Disabled
○	E1:1/7	E1 port 1/7	E1	Disabled
○	E1:1/8	E1 port 1/8	E1	Disabled
○	E1:1/9	E1 port 1/9	E1	Disabled
○	E1:1/10	E1 port 1/10	E1	Disabled
○	E1:1/11	E1 port 1/11	E1	Disabled
○	E1:1/12	E1 port 1/12	E1	Disabled
○	E1:1/13	E1 port 1/13	E1	Disabled
○	E1:1/14	E1 port 1/14	E1	Disabled
○	E1:1/15	E1 port 1/15	E1	Disabled
○	E1:1/16	E1 port 1/16	E1	Disabled
○	E1:1/17	E1 port 1/17	E1	Disabled
○	E1:1/18	E1 port 1/18	E1	Disabled
○	E1:1/19	E1 port 1/19	E1	Disabled
○	E1:1/20	E1 port 1/20	E1 (Traffic)	Disabled
○	E1:1/21	E1 port 1/21	E1 (Traffic)	Disabled

Data Refreshed on - Friday, May 11, 2007 10:40:45 AM

http://192.168.168.151 - Port Properties - Mozilla...

Port Properties:

Port: ST:1/1
Name: STM-1 port 1/1
Type: SDH
Admin Status: ● Enabled ○ Disabled ○ Testing
Oper Status: IS
Scrambler: Enabled
Loopback Status: No Loopback
J0 Trace: ○ Enabled ● Disabled
Expected Trace:
Transmitted Trace:
Received Trace:
RS Error Insertion: ● Off ○ B1 ○ LOF
MS Error Insertion: ● Off ○ B2 ○ MS-AIS
ALS Mode: Disabled
ALS Pulse Recovery Interval: 100 sec
ALS Pulse Recovery Width: 2 sec
Laser Config: ● On ○ Off
Laser Status: On

Figure 28. Enabling an STM-1 Port

Note The operational status (**Oper Status**) for an STM-1 port is **IS** (in service) when the port **Admin Status** is **Enabled** and no alarms are present at the RS and MS layers. Otherwise, the **Oper Status** for the port indicates **OOS** (out of service).

Disabling an STM-1 Port

To disable an STM-1 port from service, see Figure 28 and follow these steps:

1. In the **Port Properties** window, set **Admin Status** to **Disabled**.
2. Click on **Apply** and then on **Close** to close the window.

On the **Ports** page, **Admin Status** for the selected STM-1 port should now read **Disabled**.

Note When an STM-1 port is disabled, no port-related alarms are reported. PM data collection is also suspended. Furthermore, the disabled port transmits MS-AIS over the physical line interface.

Configuring the J0 Trace

To configure the J0 trace message for the STM-1 port, see Figure 28 on page 77 and follow these steps:

1. In the **Port Properties** window, set the **J0 Trace** to **Enabled**.
2. Type the **Expected Trace** and the **Transmitted Trace** using up to 15 ASCII characters for each field.

Note The system inserts the transmitted trace into the outgoing J0 byte for the port.

3. Click on **Apply** and then on **Close** to close the window.

Note The system does not allow enabling the J0 trace with the expected trace and transmitted trace fields empty. The system automatically enables the detection of the RS-TIM defect when J0 Trace is set to Enabled and the Expected Trace contains one or more ASCII characters. The system displays the Received Trace message if any is being received from the incoming J0 byte for the port.

Configuring the Automatic Laser Shutdown (ALS) Function

The system supports the automatic laser shutdown (ALS) function in accordance with G.958. The ALS function works in three modes: Auto, Manual Restart and Manual Restart for Test. By default, the ALS function is disabled.

When the ALS function is disabled, the system lets you manually turn the STM-1 laser on or off.

To configure the laser for manual on/off operation, see Figure 28 on page 77 and follow these steps:

1. In the **Port Properties** window, set the **Laser Config** to **On** or **Off**.
2. Click on **Apply** and then on **Close** to close the window.

Note The **Laser Status** indicates the current operation status of the laser: **On** or **Off**. The laser may be in the “on” or “off” state as a result of manual configuration or because of the application of the ALS function.

Auto Mode

In Auto mode, the transmit laser of the STM-1 port automatically shuts down when the receiver side of the port detects a loss-of-signal (LOS) condition for more than 0.5 seconds. After this event, the system periodically waits for 100-300 seconds and sends an optical pulse of 2-10 seconds of width to try recovering normal operation over the fiber link. If the link is restored and the STM-1 port on the other side of the link is also configured in ALS Auto mode, the successful reception of the optical pulse restarts the associated laser for continuous operation. This event, in turn, restarts the laser on the other side of the link and results in the recovery of normal operation over both sides of link.

To enable and configure the ALS function for the STM-1 port in Auto mode, see Figure 28 on page 77 and follow these steps:

1. In the **Port Properties** window, set the **ALS Mode** to **Auto**.

By default, the **ALS Pulse Recovery Interval** is set to 100 seconds. You can change this parameter to any valid value in the range of 100-300 seconds.

By default, the **ALS Pulse Recovery Width** is 2 seconds. You can change this parameter to any valid value in the range of 2-10 seconds.

2. Click on **Apply** and then on **Close** to close the window.

Manual Restart Mode

In Manual Restart mode, the system allows you to restart the laser manually at any time without having to wait for the completion of the pulse recovery interval. The system can enter the Manual Restart mode only when the STM-1 port was previously configured in Auto mode and the laser is shut down by the ALS function.

To configure the ALS function in Manual Restart mode, see Figure 35 and follow these steps.

1. In the **Port Properties** window, set the **ALS Mode** to **Manual**.
2. Click on the **Activate ALS Manual Command**.

At this time, the STM-1 port sends a single optical pulse with a width set by the **ALS Pulse Recovery Width**. In Manual Restart mode, the **ALS Pulse Recovery Interval** has no meaning, because the system sends only one optical pulse when the command is applied.

3. Click on **Apply** and then on **Close** to close the window.

Manual Restart for Test Mode

In Manual Restart for Test mode, the system works in the same way as the Manual Restart mode, except that the width of the opical pulse is fixed to 90 seconds. In this mode, both the **ALS Pulse Recovery Width** and the **ALS Pulse Recovery Interval** parameters have no meaning, because the system sends only one pulse of fixed duration when the command is applied.

Configuring the STM-1 in Linear 1+1 MSP Protection Mode

The STM-1 interfaces can be provisioned either as protected or unprotected.

> **Note** The factory default for the STM-1 protection mode is unprotected.

The system supports two protection modes when using Linear 1+1 MSP:

- unidirectional, non-revertive (default)
- unidirectional, revertive

> **Note** When the STM-1 interface is provisioned for Linear 1+1 MSP, the factory default is unidirectional, non-revertive.

To configure an STM-1 port for protection, see Figure 29 on page 81 and follow these steps:

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select the **Protection** folder.
3. From the expanded **Protection** folder, select the **Linear 1+1 MSP** folder.
4. From the expanded **Linear 1+1 MSP** folder, select **Settings**.
5. On the **Linear 1+1 MSP** page, select **Create 1+1 MSP**.
6. In the **Linear 1+1 MSP Provisioning** window, select the **STM-1 Working Port** and **Protection Port** pair from the available list of ports using the scroll-down button, click on **Apply** and then on **Close** to close the window.

This action completes the provisioning process using the default MSP parameters.

On the **Linear 1+1 MSP** page, the table now contains an entry with a summary of the provisioned parameters.

To configure the system for revertive switching, see Figure 29 on page 81 and follow these steps:

> **Note** After the failed direction on the working port returns to normal, revertive switching causes the system to wait for a preset amount of time (that is, the Wait-to-Restore time) before the selector on the receive side switches back from the protection port to the working port.

1. On the **Linear 1+1 MSP** page, click on **Properties**.
2. In the **Linear 1+1 MSP Properties** window, select **Revertive**.

To change the Wait-to-Restore time, continue with Step 3; otherwise, go directly to Step 5 to complete this task.

> **Note** The Wait-to-Restore time applies only when using revertive switching. Its value is ignored when using non-revertive switching.

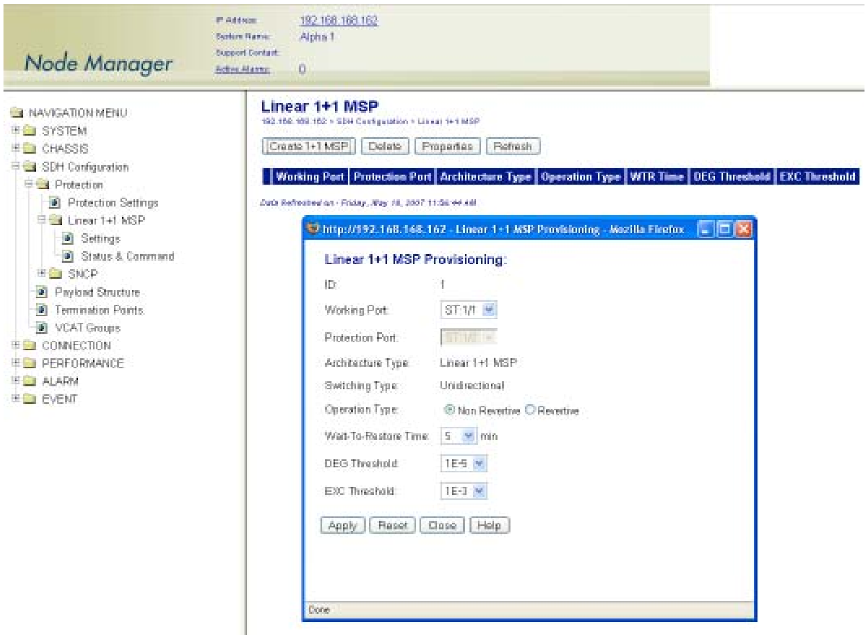
3. In the **Linear 1+1 MSP Properties** window, change the **Wait-To-Restore Time** from the factory default setting of **5** (minutes) to any integer between **0** and **12** minutes.

To change the BER settings for the detection of Signal Degrade (DEG) and Excessive Errors (EXC) at the STM-1 MS layer, continue with Step 4; otherwise, go directly to Step 5 to complete this task.

4. In the **Linear 1+1 MSP Properties** window, select the desired BER setting using the DEG (or EXC) Threshold scroll-down button.

5. Click on **Apply** and then on **Close** to close the window.

At this point, the table entry on the **Linear 1+1 MSP** page reflects any recent configuration changes.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Linear 1+1 MSP

192.168.168.162 > SDH Configuration > Linear 1+1 MSP

Data Refreshed on - Friday, May 18, 2007 11:56:44 AM

http://192.168.168.162 - Linear 1+1 MSP Provisioning - Mozilla Firefox

Linear 1+1 MSP Provisioning:

ID: 1
Working Port: ST 1/1
Protection Port: ST 1/2
Architecture Type: Linear 1+1 MSP
Switching Type: Unidirectional
Operation Type: ● Non Revertive ○ Revertive
Wait-To-Restore Time: 5 min
DEG Threshold: 1E-5
EXC Threshold: 1E-3

Figure 29. Enabling and Configuring 1+1 MSP Protection

External Commands for 1+1 MSP Switching

The system allows the use of external commands to switch between working and protection ports.

Table 27 provides a list of the external commands that the system supports:

Table 27. External Commands for 1+1 MSP Switching

Priority	Command	Action	Completion
1	Clear	Clears all switch commands	Always
2	Lockout	Disables a switch to the protection port	Always
3	Forced to Protection	Switches from the working to the protection port	Denied if the SF condition is present on the protection port or if the Lockout command is present
	Forced to Working	Switches from the protection to the working port	Denied if the Lockout command is present

Table 27. External Commands for 1+1 MSP Switching

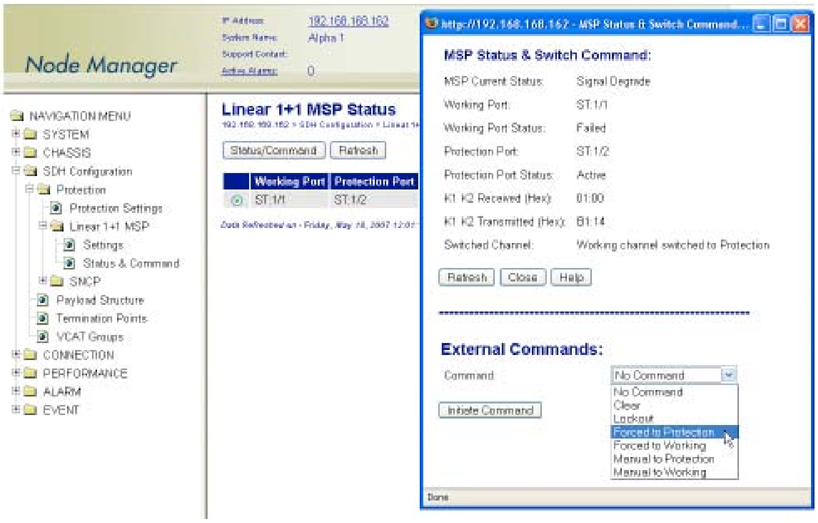
Priority	Command	Action	Completion
4	Manual to Protection	Switches from the working to the protection port	Denied if the SF or SD condition is present on the protection port or if the Lockout or Forced command is present
	Manual to Working	Switches from the protection to the working port	Denied if the SF or SD condition is present on the working port or if the Lockout or Forced command is present

To activate any of the external commands for 1+1 MSP switching, see Figure 37 and follow these steps:

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select the **Protection** folder.
3. From the expanded **Protection** folder, select the **Linear 1+1 MSP** folder.
4. From the expanded **Linear 1+1 MSP** folder, select **Status & Command**.
5. On the **Linear 1+1 MSP Status** page, select the table entry and click on **Status/Command**.
6. In the **MSP Status & Switch Command** window, use the scroll-down button to select one of the **Command** options in Table 27.

> **Note** By default, **Command** is set to **No Command**. The **MSP Status & Switch Command** window also displays the current status of the protection group, including the transmitted and received values for the K1 and K2 bytes and the status of the protection switch selector.

7. Click on **Initiate Command** to activate the external command.
8. To reset any active command, select the **Clear** command option and click on **Initiate Command**. Otherwise, the current command remains active until a higher priority command is issued or failure event occurs (see Table 27 on page 81).



Node Manager

IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Linear 1+1 MSP Status

192.168.168.162 > SDH Configuration > Linear 1+

	Working Port	Protection Port
●	ST:1/1	ST:1/2

Data Refreshed on - Friday, May 18, 2007 12:0

http://192.168.168.162 - MSP Status & Switch Command...

MSP Status & Switch Command:

MSP Current Status: Signal Degrade
Working Port: ST:1/1
Working Port Status: Failed
Protection Port: ST:1/2
Protection Port Status: Active
K1 K2 Received (Hex): 01:00
K1 K2 Transmitted (Hex): B1:14
Switched Channel: Working channel switched to Protection

External Commands:

Command: No Command

Done

Figure 30. Configuring the External 1+1 MSP Protection Switch Commands

Configuring the SDH Payload Structure

The OnSite OS-10 system allows you to configure the STM-1 to carry any standards-based combination of VC-4, VC-3 and VC-12 payloads. The system uses a simple, standards-based index to help you identify the location of SDH structures within the STM-1 port. All SDH structures are uniquely identified by four letters, as indicated in Table 28.

Table 28. Index Letters to Identify SDH Structures

Letter	Indicates the Location of
U	AU-4 (VC-4) within the STM-1
K	TUG-3 within a VC-4
L	TUG-2 within a TUG-3
M	TU-12 within a TUG-2

Table 29 summarizes the structures and ranges represented by the index.

Table 29. Provisioning Range for SDH Structures

Index Letter	SDH Structures			Provisioning Range
U	AUG-1	AU-4	VC-4	1
K	TUG-3	TU-3	VC-3	1 to 3
L	TUG-2	TU-2*	VC-2*	1 to 7
M	–	TU-12	VC-12	1 to 3

As shown in Table 29, the same index is shared by a number of SDH structures.

Note Because only one AU-4 exists within the STM-1, the value of U is always 1. TU-2 and VC-2 structures are not supported in the system but are included in Table 36 for illustration purposes and completeness. Most, if not all, SDH equipment to which the OS-10 connects does not support switching and connectivity at this level.

Figure 31 shows the subdivision of payload structures within an STM-1 for the case in which TUG-3 No. 2 contains seven TUG-2 groups, and each TUG-2 group contains three TU-12 time slots.

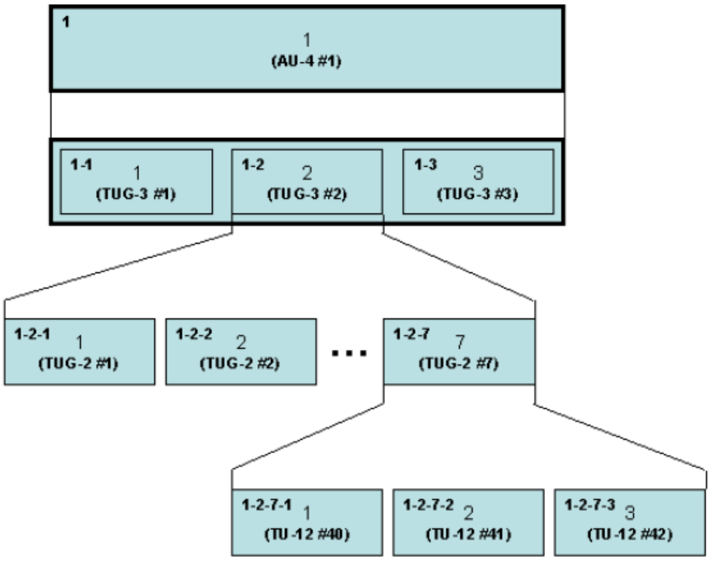


Figure 31. Subdivision of STM-1 Payload Structures

The Web-based management interface uses the notation in Figure 39 to help you identify and locate SDH structures within the STM-1.

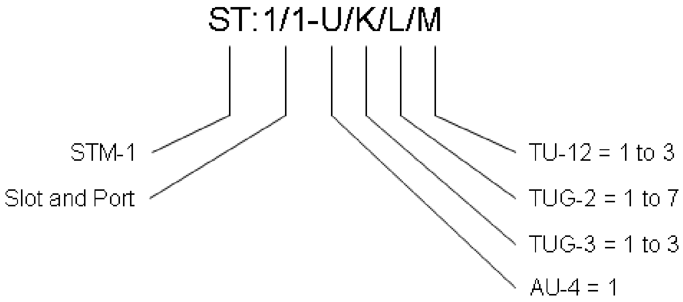


Figure 32. Notation for SDH Structures within the OnSite OS-10-series STM-1 Interfaces

Table 30 shows the default configuration for the STM-1 payload structure.

Table 30. Default SDH Payload Structure

STM-1 Port No.	AU-4/VC-4 No.	TUG-3 No.	Default Payload
1 and 2	1	1	TU-12
		2	TU-12
		3	TU-12

Note A TUG-3 contains 21 TU-12 time slots when configured for TU-12 transport. A TUG-3 contains a single TU-3 time slot when configured for TU-3 transport.

To change the STM-1 payload structure, see Figure 40 and follow these steps:

Note The payload structure defines the available set of TU-3 and TU-12 time slots into which you can connect client ports mapped to VC-3 and VC-12 termination points.

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select **Payload Structure**.

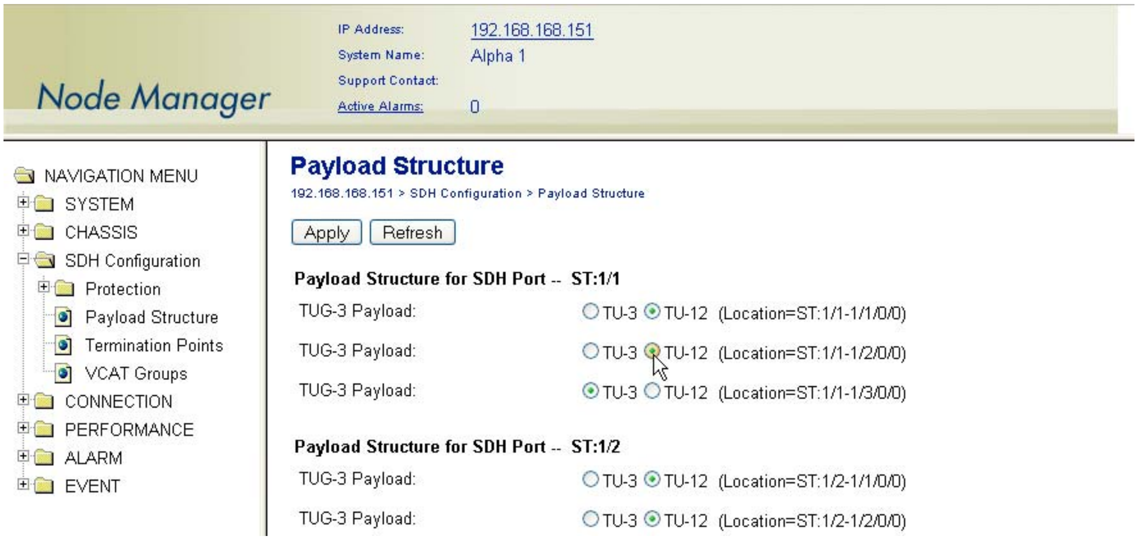
At this point, the **Payload Structure** page displays a table with the current payload type for each of the TUG-3 locations within the VC-4. Each TUG-3 has a unique location index. For instance, the notation ST:1/1-1/3/0/0 indicates the location of TUG-3 number 3 (K=3) within VC-4 number 1 (U=1) in STM-1 slot 1 port 1. The indexing numbers L and M are zero to indicate no further subdivisions below TUG-3.

3. On the **Payload Structure** page, set the payload type for each TUG-3 location to **TU-3** or **TU-12**.
4. Click on **Apply** to complete this task.

Note The system does not allow configuration of a TUG-3 to TU-3 if any TU-12 time slot is being used in a connection (see §9.3). You would need to first delete all TU-12 connections from the TUG-3 before you can change the payload configuration to TU-3.

- The system generates the unequipped signal for any TU-3 or TU-12 time slot that is not connected to a client port mapped to a VC-3 or VC-12 termination point. The unequipped signal consists of a valid TU pointer and an “all-zeros” VC-3 or VC-12 payload.

- The payload structure for STM-1 port 1 and port 2 is the same when the ports are configured as a protected pair using Linear 1+1 MSP.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Payload Structure

192.168.168.151 > SDH Configuration > Payload Structure

Payload Structure for SDH Port -- ST:1/1

TUG-3 Payload: ○ TU-3 ● TU-12 (Location=ST:1/1-1/1/0/0)
TUG-3 Payload: ○ TU-3 ● TU-12 (Location=ST:1/1-1/2/0/0)
TUG-3 Payload: ● TU-3 ○ TU-12 (Location=ST:1/1-1/3/0/0)

Payload Structure for SDH Port -- ST:1/2

TUG-3 Payload: ○ TU-3 ● TU-12 (Location=ST:1/2-1/1/0/0)
TUG-3 Payload: ○ TU-3 ● TU-12 (Location=ST:1/2-1/2/0/0)

Figure 33. Configuring the STM-1 Payload Structure

SDH and Client Port Connections

The system supports the following types of connections:

- 2-way (bidirectional)
- 1-way (unidirectional)
- 1-way drop-and-continue
- 2-way drop-and-continue
- 1-way multicast

The following sections provide an overview of each type of connection.

2-way Connections

By default, the system uses 2-way connections to connect traffic between STM-1 ports and client signal ports (E1/T1, E3/DS3 and Ethernet). Figure 34 shows examples of 2-way add-drop connections between E1 client signal ports and unprotected TU-12 timeslots. As shown in the figure, the E1 port can be connected to an unprotected TU-12 on either STM-1 port 1 (west) or port 2 (east). The figure also shows an example of a 2-way cross-connection between TU-12 timeslots on STM-1 port 1 (west) and 2 (east).

Note that each connection point has two components: a source (So) and a sink (So). The So side is where the connection originates and the Sk side is where the connection terminates. To set up a 2-way connection, is only necessary to identify one of the connection points as the So and the other as the Sk.

Which of the two connection points is identified as the So or the Sk is not important. The 2-way relationship between the two connection points binds the So and Sk sides for each connection point together.

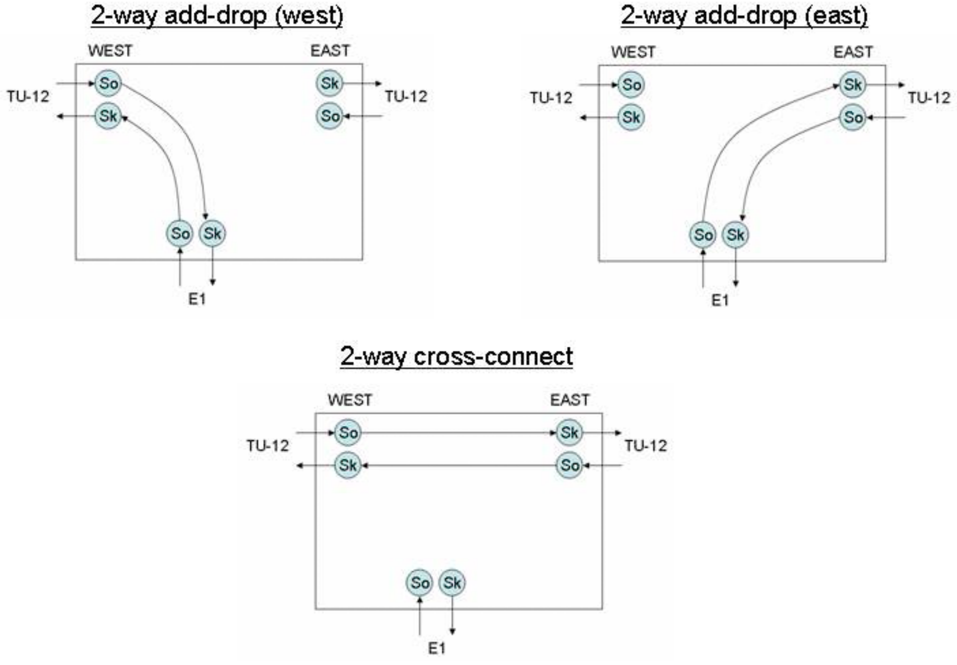


Figure 34. Unprotected 2-way Connections (Examples)

Figure 35 shows examples of 2-way add-drop connections between E1 client signal ports and protected TU-12 timeslots using MSP 1+1 or SNCP.

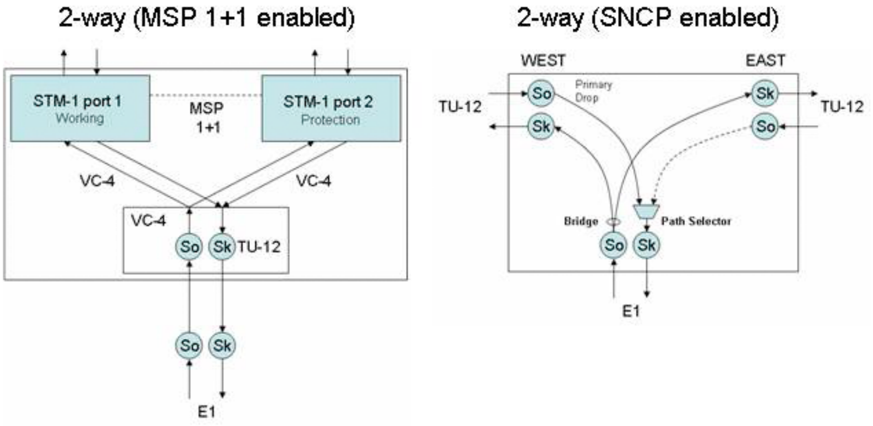


Figure 35. Protected 2-way Connections (Examples)

The system supports 2-way connections at the E1 and T1 levels using TU-12 timeslots; at the E3 and DS3 levels using TU-3 timeslots; and at the Ethernet level using VCAT groups (VCGs).

1-way Connections

Figure 36 shows an example of a 1-way “add” connection between an E1 port and a TU-12 timeslot. For 1-way “add” connections, the activation of SNCP protection creates a 1-by-2 bridge between the So and the Sk points of the connection. In the example of Figure 43, the bridge exists between the source E1 port and the sink TU-12 timeslot on the east and west STM-1 ports.

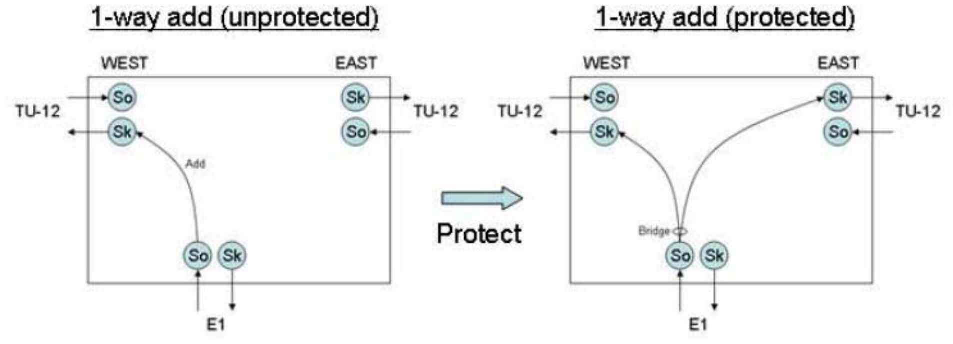


Figure 36. 1-way Add Connections (Examples)

Note The system declares an LP-UNEQ condition at the VC-12 level if an E1 or T1 port is the source of a 1-way connection and the sink component of the port remains unconnected to a VC-12 path at the far end. This LP-UNEQ condition results in the generation of LP-RDI by the source point of the port. Likewise, the system declares an LP-UNEQ condition and generates LPRDI at the VC-3 level if a DS3 or

E3 port is the source of a 1-way connection and the sink component of the port remains unconnected to a VC-3 path at the far end. Also, for an Ethernet flow that originates a 1-way connection to a VCG, LP-UNEQ detection and LP-RDI generation occurs for all VCG members that remain unconnected at the sink point to VC-3 or VC-12 paths at the far end.

Figure 37 shows an example of a 1-way "drop" connection between an E1 port and a TU-12 timeslot. For 1-way "drop" connections, the activation of SNCP protection creates a path selector between the So and Sk points of the connection. In the example of Figure 44, the path selector exists between the source TU-12 timeslot on the east and west STM-1 ports and the E1 port at the sink.

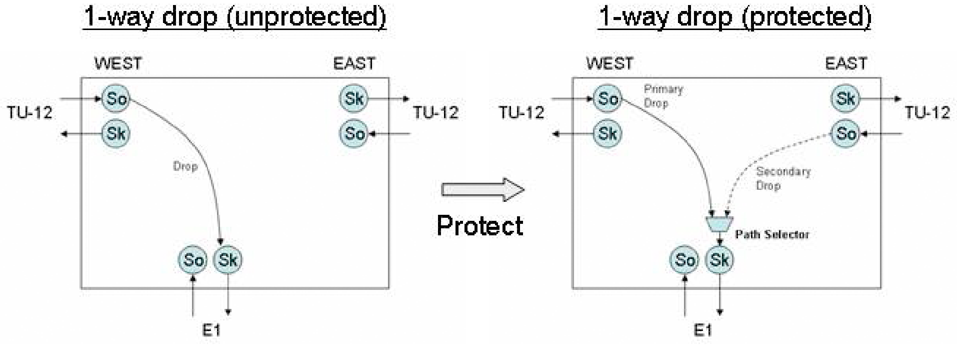


Figure 37. 1-way Drop Connections (Examples)

The system supports 1-way connections at the E1 and T1 levels using TU-12 timeslots; at the E3 and DS3 levels using TU-3 timeslots; and at the Ethernet level using VCAT groups (VCGs).

Drop-and-Continue Connections

The system supports two types of drop-and-continue connections: 1-way and 2-way drop-and-continue. Figure 38 on page 89 shows an example of a 1-way drop-and-continue connection at the E1 level. In a 1-way E1 drop-and-continue connection from west, the system drops a TU-12 timeslot from the west port (STM-1 port 1) into an E1 port while a copy of the VC-12 payload on the TU-12 continues onwards to the same TU-12 location on the east port (STM-1 port 2). When SNCP is enabled for a 1-way drop-and-continue connection from west, the system makes a similar connection from the east port and turns on a path selector function that uses the drop side from the west as the primary drop path and the drop side from the east as the secondary drop path. Likewise, Figure 38 shows an example of a 1-way E1 drop-and-continue connection from east.

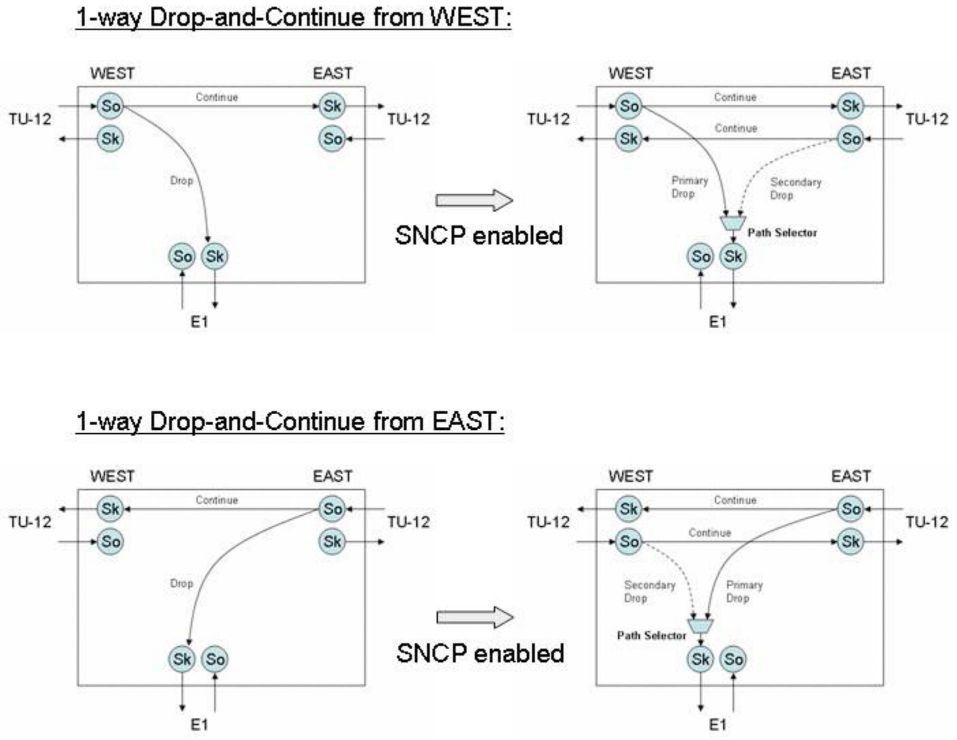


Figure 38. 1-way Drop-and-Continue Connections (Examples)

Figure 39 on page 90 shows an example of a 2-way drop-and-continue connection at the E1 level. In contrast to 1-way E1 drop-and-continue connections, 2-way E1 drop-and-continue connections support 2-way transmission between a TU-12 timeslot and an E1 port while a copy of the VC-12 payload on the TU-12 continues onwards to the same TU-12 location on the other STM-1 port. As Figure 46 shows, when SNCP is enabled for a 2-way drop-and-continue connection from west, the system turns on a path selector function that uses the drop side from west as the primary drop path and the drop side from the east as the secondary drop path. There is no "continue" component from the east port (as in 1-way drop-andcontinue connections) because the "add" part of the connection from the E1 port occupies the corresponding TU-12 on the west port. Likewise, Figure 39 shows an example of a 2-way E1 drop-andcontinue connection from the east port.

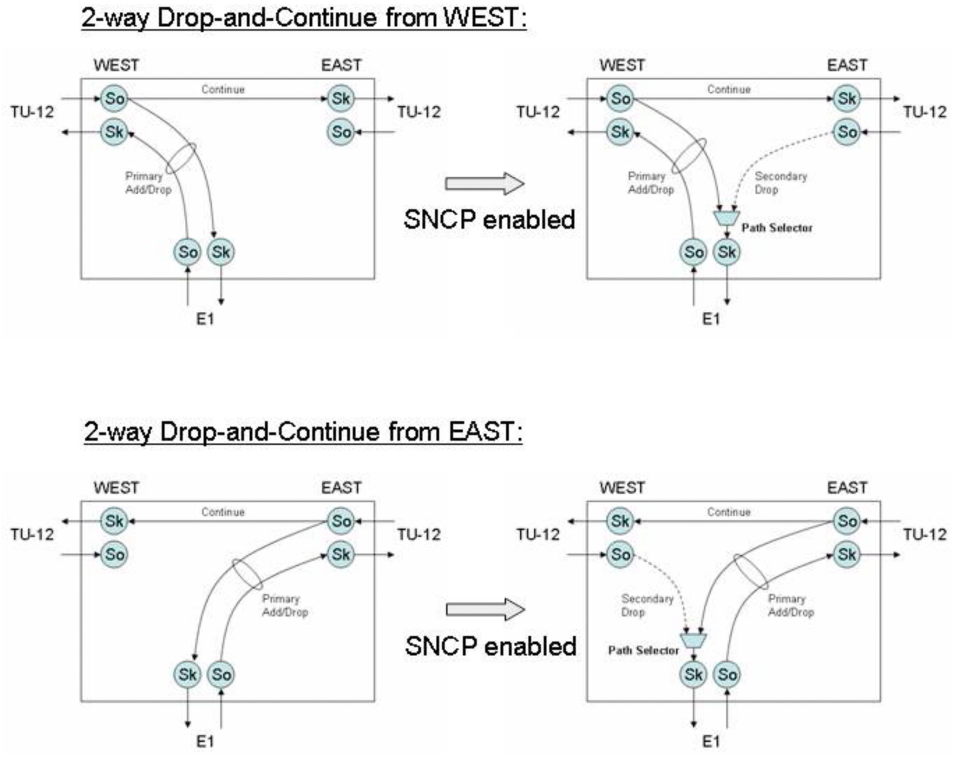


Figure 39. 2-way Drop-and-Continue Connections (Examples)

The system supports drop-and-continue connections at the E1 and T1 levels using TU-12 timeslots; at the E3 and DS3 levels using TU-3 timeslots; and at the Ethernet level using VCAT groups (VCGs).

Multicast Connections

The system supports multicast connections at the E1 and T1 levels using TU-12 timeslots; at the E3 and DS3 levels using TU-3 timeslots; and at the Ethernet level using VCAT groups (VCGs). The system also supports multicast connections at the VC-12 level between TU-12 timeslots, and at the VC-3 level between TU-3 timeslots.

As shows, for an E1 multicast connection from west, the system drops a TU-12 timeslot on the west port into a single E1 port. At this point, the multicast connection with a single leg (Leg 1) looks the same as an unprotected 1-way drop connection (see Figure 44). However, because the initial leg is part of a multicast connection, you can create additional multicast legs (Legs 2 and 3 in Figure 47) to connect the same TU-12 timeslot to other E1 ports in the system. The system does place restrictions on the maximum number of multicast legs originating from one TU-12, as long as there are E1 or TU-12 sink points available.

When SNCP is enabled for a 1-way multicast connection from west, the system turns on a path selector function that uses the drop side from west as the primary drop path and the drop side from the east as the secondary drop path. Note that the system applies the SNCP path selector to only one TU-12 timeslot, and that the selected path (east or west) becomes the source for all multicast legs.

Note To provide the equivalent function of a combined 1-way multicast and drop-and-continue connection, you can create an additional leg between the TU timeslots on the east and west ports.

Figure 40 also provides an example of a multicast connection at the Ethernet level. In contrast to multicast connections at the E1/T1 or E3/DS3 level, multicast connections at the Ethernet level occur at the packet level within the high-density Ethernet (HD-ENET) expansion module.

Once the system makes the first multicast connection from a VCG into an Ethernet port on the HD-ENET module (Leg 1), you can create additional multicast legs (see Legs 2 and 3 in Figure 40) to connect the same Ethernet flow from the VCG to other Ethernet ports in the module. The system does place restrictions on the maximum number of multicast legs originating from one VCG, as long as there are Ethernet flow sink points available in the module.

When SNCP is enabled for a 1-way multicast connection from a VCG, the system turns on a path selector function for each member of the VCG. The selected path (east or west) for each member becomes part of the VCG that originates all multicast legs at the Ethernet level.

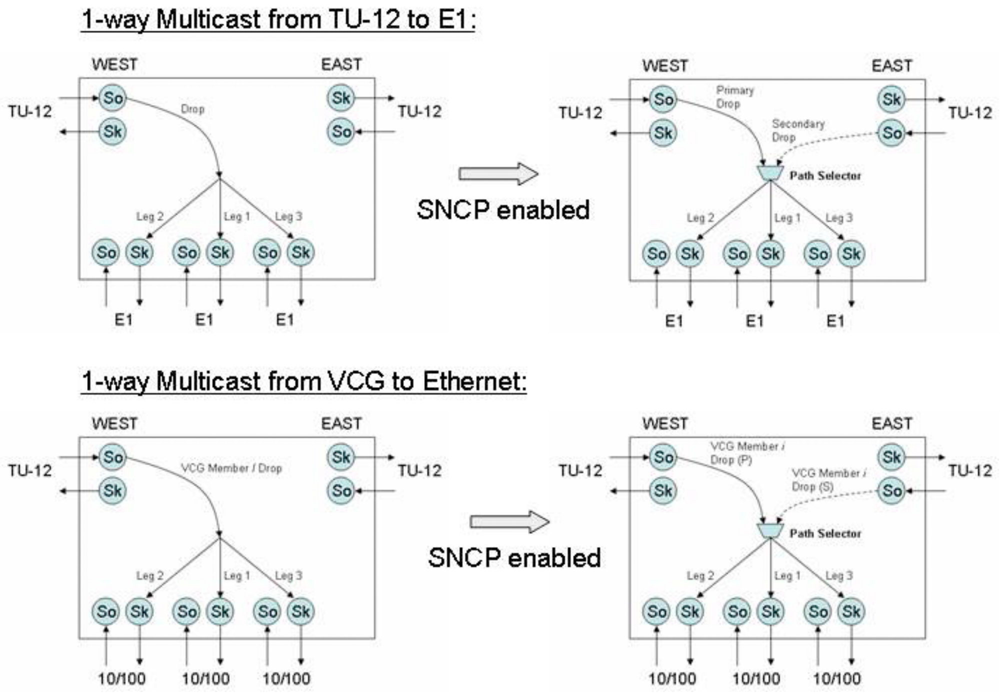


Figure 40. 1-way Multicast Connections (Examples)

SDH Alarms

The system monitors SDH alarms according to Recommendations G.707, G.783 and G.826. The following sections provide the procedures for monitoring active SDH alarms, changing the alarm severity, and displaying the alarm log.

Note The system declares and displays an alarm condition if a defect persists for 2.5 ± 0.5 seconds. The alarm condition is cleared when the defect is terminated and remains absent for 10 ± 0.5 seconds.

Monitoring SDH Alarms

Table 31 provides a list of the SDH alarms that the system supports.

Table 31. SDH Alarms

Monitored Entity	Near-end Alarm	Description	Far-end Alarm	Description
STM-1 RS	LOS	Loss of Signal		
	LOF	Loss of Frame		
	RS-TIM	Trace identifier mismatch		
STM-1 MS	MS-AIS	Alarm Indication Signal	MS-RDI	Remote Defect Indication
	MS-EXC	Excessive Errors		
	MS-DEG	Degraded Signal		
AU-4	AU-AIS	Alarm Indication Signal		
	AU-LOP	Loss of Pointer		
VC-4	HP-UNEQ	Unequipped	HP-RDI	Remote Defect Indication
	HP-PLM	Path Label Mismatch		
	HP-TIM	Trace identifier mismatch		
TU-3 and TU-12	TU-AIS	Alarm Indication Signal		
	TU-LOP	Loss of Pointer		
	TU-LOM	Loss of Multiframe		
VC-3 and VC-12	LP-UNEQ	Unequipped	LP-RDI	Remote Defect Indication
	LP-PLM	Path Label Mismatch		
	LP-TIM	Trace identifier mismatch		

Note The system declares an MS-EXC (excessive errors) condition when the measured BER (bit error rate) exceeds a provisioned value. The BER is calculated based on the results of the B2 byte at the MS layer. The supported BER thresholds for declaring MS-EXC are: 10-5, 10-4, and 10-3. (10-3 is the default.) The system initiates a protection switch upon detecting MS-EXC. This applies only to systems configured for 1+1 operation.

Note The system declares an MS-DEG (degraded signal) condition when the measured BER exceeds 10-6 (default setting). The supported BER thresholds for declaring MS-DEG are: 10-9, 10-8, 10-7, 10-6, and 10-5. (10-6 is the default.) The system initiates a protection switch upon detecting MS-DEG. This applies only to systems configured for 1+1 operation.

The front panel provides an alarm status LED for each STM-1 port (port 1 and port 2) to indicate the presence of an active alarm condition of any severity level (Critical, Major, Minor, or Warning). The LED is lit according to the color codes in Table 32.

Table 32. STM-1 Alarm Status LED

LED Color	Description
Green	No alarm is present on the STM-1 port.
Amber	An alarm is present on the STM-1 port.
Off	The STM-1 port is disabled.

To display SDH alarms, if present, see Figure 48 and follow these steps:

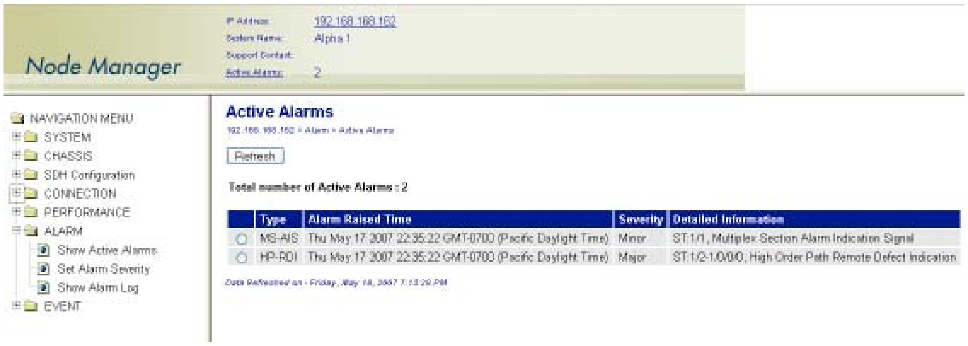
1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Show Active Alarms**.

At this point, the **Active Alarms** page displays all active alarms in the system, including SDH alarms, if present. The table contains a separate entry for each active SDH alarm. Table 33 describes the fields for each SDH alarm entry.

Table 33. Table Entries for Active SDH Alarms

Table Entry for Active Alarms	Field Value
Type	See Table 31 on page 92 for a complete list of SDH alarms.
Alarm Raised Time	Date and time
Severity	Critical, Major, Minor, or Warning
Detailed Information	Location of affected SDH entity (ST:*slot/port* or ST:*slot/port-U/K/L/M*)

Note The system automatically updates the Active Alarms page every 60 seconds. Click on Refresh if you need to update the table with the most recent active alarm information. Individual table entries automatically clear whenever previously active alarms are no longer present.



IP Address: 192.168.188.162
System Name: Alpha 1
Support Contact:
Active Alarms: 2

Active Alarms

192.168.188.162 > Alarm > Active Alarms

Total number of Active Alarms : 2

	Type	Alarm Raised Time	Severity	Detailed Information
○	MS-AIS	Thu May 17 2007 22:35:22 GMT-0700 (Pacific Daylight Time)	Minor	ST:1/1, Multiplex Section Alarm Indication Signal
○	HP-RDI	Thu May 17 2007 22:35:22 GMT-0700 (Pacific Daylight Time)	Major	ST:1/2-1/0/0/0, High Order Path Remote Defect Indication

Data Refreshed on - Friday, May 18, 2007 7:13:29 PM

Figure 41. Displaying SDH Alarms

Changing SDH Alarm Default Severities

The system allows changing the default severity of any given SDH alarm condition. Alarm severities are the following:

- Critical
- Major
- Minor
- Warning

Table 34 provides the default severities for SDH alarms:

Table 34. SDH Alarm Default Severities

Monitored Entity	Near-end Alarm	Default Severity	Far-end Alarm	Default Severity
STM-1 RS	LOS	Critical		
	LOF	Critical		
	RS-TIM	Major		
STM-1 MS	MS-AIS	Major	MS-RDI	Major
	MS-EXC	Major		
AU-4	AU-AIS	Major		
	AU-LOP	Major		
VC-4	HP-UNEQ	Critical	HP-RDI	Major
	HP-PLM	Critical		
	HP-TIM	Major		
TU-3 and TU-12	TU-AIS	Major		
	TU-LOP	Critical		
	TU-LOM	Critical		
VC-3 and VC-12	LP-UNEQ	Critical	LP-RDI	Major
	LP-PLM	Critical		
	LP-TIM	Critical		

To change the default severity for supported SDH alarms, see Figure 42 on page 95 and follow these steps:

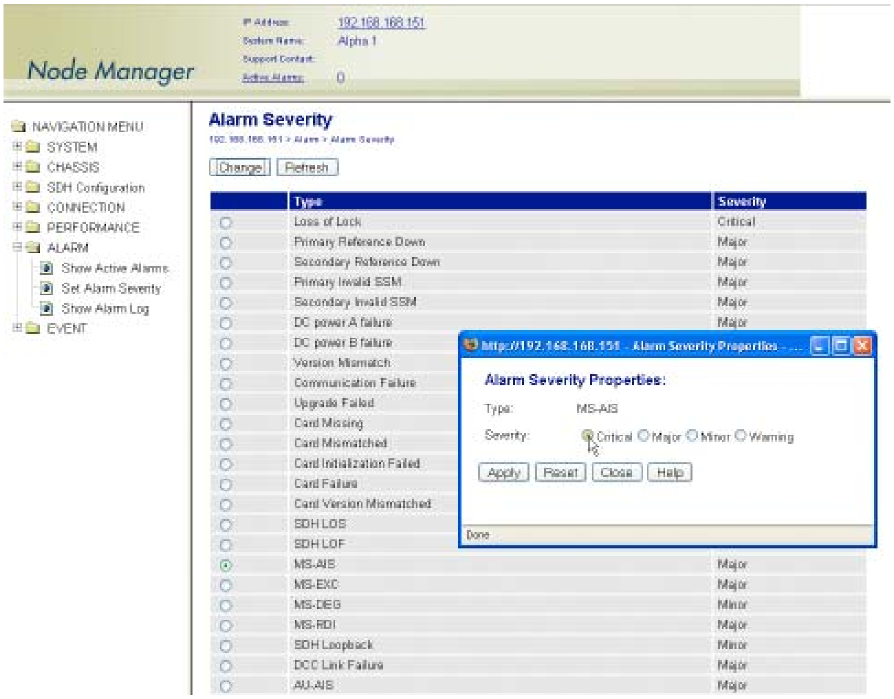
1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Set Alarm Severity**.

At this point, the Alarm Severity page displays a table with all supported system alarms.

3. Select the table entry containing the SDH alarm **Type** and click on **Change**.
4. In the **Alarm Severity** window, set **Severity** to any desired level (Critical, Major, Minor, or Warning).
5. Click on **Apply** and then on **Close** to close the window.

On the **Alarm Severity** page, the **Severity** for the selected SDH alarm **Type** should now reflect the change in the reported severity level.

Note The change applies to all monitored entities for a particular SDH layer within the system. For example, changing the default severity for TU-AIS applies to all TU-3 and TU-12 within the system.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Alarm Severity

192.168.168.151 > Alarm > Alarm Severity

	Type	Severity
○	Loss of Lock	Critical
○	Primary Reference Down	Major
○	Secondary Reference Down	Major
○	Primary Invalid SSM	Major
○	Secondary Invalid SSM	Major
○	DC power A failure	Major
○	DC power B failure	
○	Version Mismatch	
○	Communication Failure	
○	Upgrade Failed	
○	Card Missing	
○	Card Mismatched	
○	Card Initialization Failed	
○	Card Failure	
○	Card Version Mismatched	
○	SDH LOS	
○	SDH LOF	
●	MS-AIS	Major
○	MS-EXC	Major
○	MS-DEG	Minor
○	MS-RDI	Major
○	SDH Loopback	Minor
○	DCC Link Failure	Major
○	AU-AIS	Major

http://192.168.168.151 - Alarm Severity Properties - ...

Alarm Severity Properties:

Type: MS-AIS

Severity: ● Critical ○ Major ○ Minor ○ Warning

Figure 42. Changing SDH Alarm Severities

Displaying the Alarm Log

To display historical alarms, including any SDH alarms if present, follow these steps:

1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Show Alarm Log**.

At this point, the **Alarm Log** page displays a list of the 50 most recent alarm messages. The system keeps up to 500 entries in the alarm log.

Note The alarm log is a FIFO (first-in fist-out) log.

Click on **Last 50 Log Entries** or **Next 50 Log Entries** to move around and display the entire contents of the log. Click on **Clear Log** if you wish to delete permanently the current log entries.

SDH Performance Monitoring

The following sections provide the procedures for displaying current and historical SDH performance monitoring (PM) data and configuring and displaying PM thresholds.

The system calculates the SDH error performance events listed inTable 35 in accordance to Recommendations G.826 and G.829.

Table 35. SDH Error Performance Events

PM Parameter	Description	Definition
BBE	Background Block Error	An EB (errored block) not part of an SES
ES	Errored Second	A second containing at least one EB or a defect
SES	Severely Errored Second	A second containing K[1] or more EBs or a defect
UAS	Unavailable Second	A period of unavailable time that begins at the onset of 10 consecutive SES

Note A period of unavailable time begins at the onset of 10 consecutive SES seconds. These 10 seconds are part of unavailable time. A period of available time begins at the onset of 10 consecutive non-SES seconds. These 10 seconds are part of available time.

Table 36 provides a list of the near-end PM parameters that the system collects at various SDH layers.

Table 36. Monitored PM Parameters at Various SDH Layers

SDH Layer	Monitored Entity	PM Parameters
RS	STM-1	BBE, ES, and SES
MS	STM-1	BBE, ES, SES, and UAS
HP	VC-4	BBE, ES, SES, and UAS
LP	VC-3 and VC-12	BBE, ES, SES, and UAS

For each PM parameter, near-end PM data is stored in the following counters:

- Current 15 minutes
- Recent 15 minutes (previous 95-by-15 minute intervals)
- Current 24 hours
- Recent 24 hours (previous day only)

Note PM event counting for BBE, ES, and SES is inhibited during unavailable time in accordance to Recommendations G.826 and G.829.

By default, the system uses the SES threshold values in Table 37.

Table 37. SDH SES Threshold Values

Monitored Entity	SES Threshold	Applicable Standard
VC-12	600 EB	G.826
VC-3	2,400 EB	G.826
VC-4	2,400 EB	G.826
STM-1 RS	2,400 EB	G.829
STM-1 MS	28,800 EB	G.829

The SES threshold value (for example, 2,400 for VC-3) is the value “K” in the definition of SES in Table 35 on page 96.

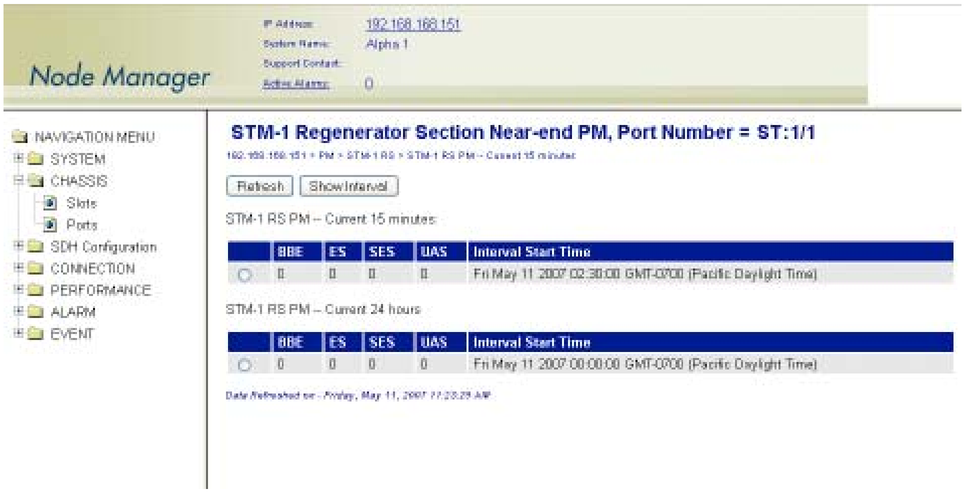
> **Note** According to G.829, PM counting at the STM-1 MS layer is based on 24 BIP-1 counts using the B2 bytes. This counting method is different from the other layers and results in up to 24 EBs per frame, and a maximum of 192,000 EBs per second.

Monitoring STM-1 Port Performance

To display current PM data for an STM-1 port, see Figure 43 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the STM-1 port being configured and click **Show PM**.

At this point, the **STM-1 Regenerator Section Near-end PM** page shows the near-end PM data for both the current 15-minute and 24-hour periods. The PM data is not updated automatically as new events occur during the Current 15-minute and 24-hour periods. Click on **Refresh** to update the tables with the most recent cumulative count for the current periods.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

STM-1 Regenerator Section Near-end PM, Port Number = ST:1/1

192.168.168.151 > PM > STM-1 RS > STM-1 RS PM - Current 15 minutes

STM-1 RS PM – Current 15 minutes

	BBE	ES	SES	UAS	Interval Start Time
○	0	0	0	0	Fri May 11 2007 02:30:00 GMT-0700 (Pacific Daylight Time)

STM-1 RS PM – Current 24 hours

	BBE	ES	SES	UAS	Interval Start Time
○	0	0	0	0	Fri May 11 2007 00:00:00 GMT-0700 (Pacific Daylight Time)

Date Refreshed on - Friday, May 11, 2007 11:23:29 AM

Figure 43. Displaying Current PM Data for an STM-1 Port

Continue with the steps below to display historical PM data.

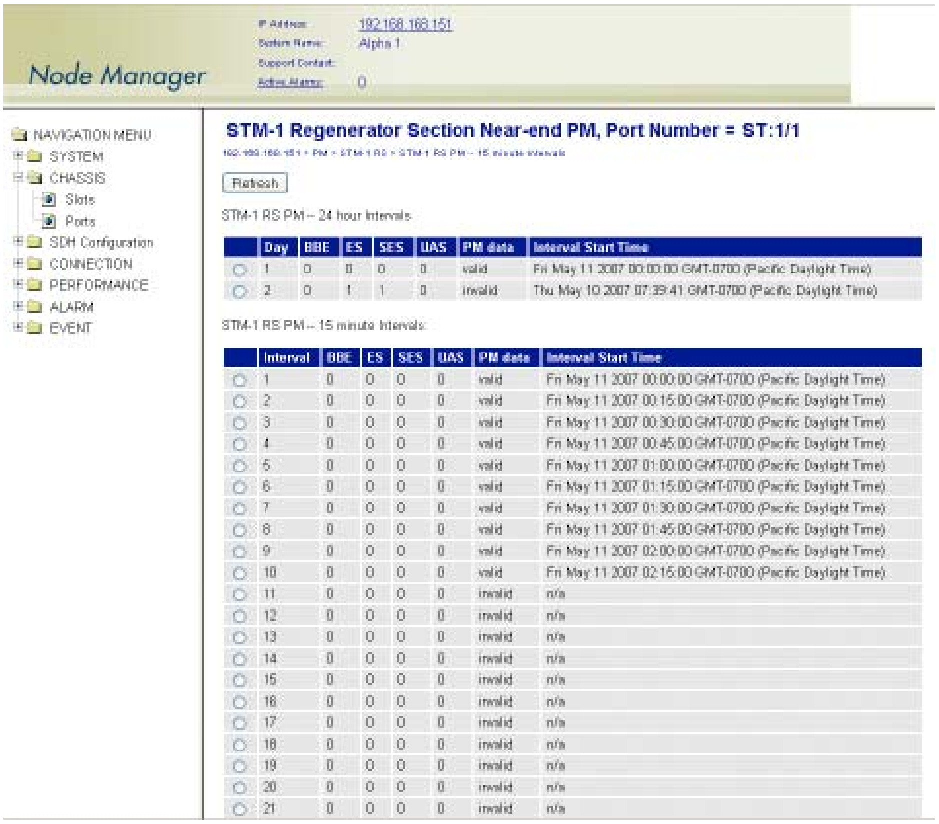
4. Click on **Show Interval**.

At this point, the **STM-1 Regenerator Section Near-end PM** page shows the near-end PM data for the following intervals (see Figure 44):

- Current plus previous 95-by-15-minute intervals (24 hours total)
- Current plus previous day (2 days total)

Click on **Refresh** to update the tables with the most recent cumulative count for the current periods. This action updates only the first entry in the tables, which corresponds to the current measurement period.

Note The tables display **Invalid** under **PM data** when the data collected during a measurement period is considered invalid. The **Interval Start Time** also displays **n/a** (not available).



STM-1 Regenerator Section Near-end PM, Port Number = ST:1/1

192.168.168.151 > PM > STM-1 RS > STM-1 RS PM -- 15 minute intervals

STM-1 RS PM -- 24 hour Intervals:

	Day	BBE	ES	SES	UAS	PM data	Interval Start Time
○	1	0	0	0	0	valid	Fri May 11 2007 00:00:00 GMT-0700 (Pacific Daylight Time)
○	2	0	1	1	0	invalid	Thu May 10 2007 07:39:41 GMT-0700 (Pacific Daylight Time)

STM-1 RS PM -- 15 minute Intervals:

	Interval	BBE	ES	SES	UAS	PM data	Interval Start Time
○	1	0	0	0	0	valid	Fri May 11 2007 00:00:00 GMT-0700 (Pacific Daylight Time)
○	2	0	0	0	0	valid	Fri May 11 2007 00:15:00 GMT-0700 (Pacific Daylight Time)
○	3	0	0	0	0	valid	Fri May 11 2007 00:30:00 GMT-0700 (Pacific Daylight Time)
○	4	0	0	0	0	valid	Fri May 11 2007 00:45:00 GMT-0700 (Pacific Daylight Time)
○	5	0	0	0	0	valid	Fri May 11 2007 01:00:00 GMT-0700 (Pacific Daylight Time)
○	6	0	0	0	0	valid	Fri May 11 2007 01:15:00 GMT-0700 (Pacific Daylight Time)
○	7	0	0	0	0	valid	Fri May 11 2007 01:30:00 GMT-0700 (Pacific Daylight Time)
○	8	0	0	0	0	valid	Fri May 11 2007 01:45:00 GMT-0700 (Pacific Daylight Time)
○	9	0	0	0	0	valid	Fri May 11 2007 02:00:00 GMT-0700 (Pacific Daylight Time)
○	10	0	0	0	0	valid	Fri May 11 2007 02:15:00 GMT-0700 (Pacific Daylight Time)
○	11	0	0	0	0	invalid	n/a
○	12	0	0	0	0	invalid	n/a
○	13	0	0	0	0	invalid	n/a
○	14	0	0	0	0	invalid	n/a
○	15	0	0	0	0	invalid	n/a
○	16	0	0	0	0	invalid	n/a
○	17	0	0	0	0	invalid	n/a
○	18	0	0	0	0	invalid	n/a
○	19	0	0	0	0	invalid	n/a
○	20	0	0	0	0	invalid	n/a
○	21	0	0	0	0	invalid	n/a

Figure 44. Displaying PM Data Intervals for an STM-1 Port

To display current and historical PM data for all STM-1 ports in the system, follow these steps:

1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select **Counters**.
3. From the expanded **Counters** folder, select **SDH**.
4. From the expanded **SDH** folder, select **STM-1 RS**.

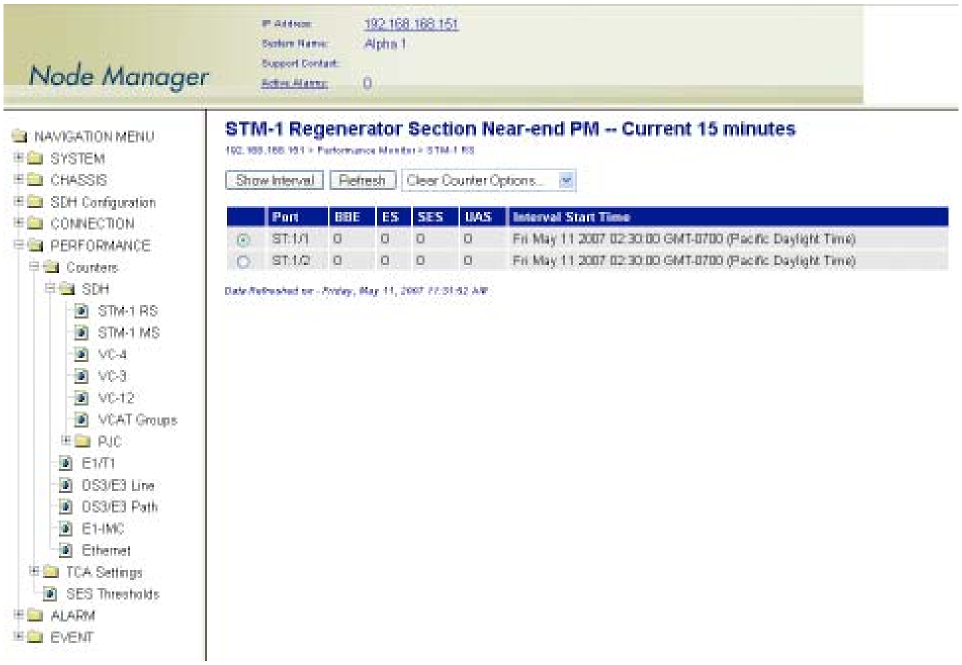
At this point, the **STM-1 Regenerator Section Near-end PM** page shows the near-end PM data for the current 15-minute period only (see Figure 45).

> **Note** You may select **STM-1 MS** instead of **STM-1 RS** in Step 4 to display the corresponding near-end PM data for the STM-1 MS layer.

Continue with the steps that follow to display historical PM data for both 15-minute and 24-hour periods.

5. Select an STM-1 port and click on **Show Interval**.

> **Note** The preceding notes for the **STM-1 Regenerator Section Near-end PM** page also apply to this procedure.



STM-1 Regenerator Section Near-end PM -- Current 15 minutes

192.168.168.151 > Performance Monitor > STM-1 RS

	Port	BBE	ES	SES	UAS	Interval Start Time
●	ST:1/1	0	0	0	0	Fri May 11 2007 02:30:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/2	0	0	0	0	Fri May 11 2007 02:30:00 GMT-0700 (Pacific Daylight Time)

Data Refreshed on - *Friday, May 11, 2007 11:31:52 AM*

Figure 45. Displaying Current PM Data for All STM-1 Ports

To clear the current PM data for an STM-1 port, see Figure 45and follow this step:

1. On the **STM-1 Regenerator Section Near-end PM** page, select one of the STM-1 port entries and use the **Clear Counter Options...** scroll-down button to select one of the available options for clearing the current 15 minute or 24 hour counters, or both.

Monitoring VC-n Performance

To display current and historical PM data for all VC-12, VC-3, or VC-4 termination points (TPs) in the system, see Figure 46 and follow these steps:

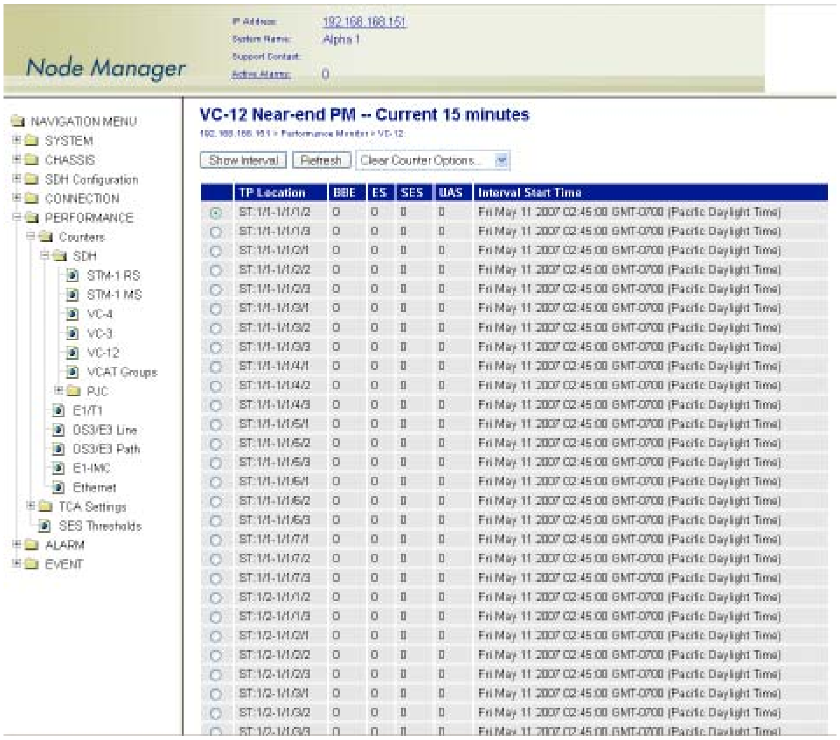
> **Note** The system displays PM data only for VC-12 or VC-3 TPs that are connected to a client port.

1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select **Counters**.
3. From the expanded **Counters** folder, select **SDH**.
4. From the expanded **SDH** folder, select **VC-12**, **VC-3** or **VC-4**.

At this point, the **VC-12**, **VC-3** or **VC-4 Near-end PM** page shows the near-end PM data for the current 15-minute period only. Figure 53 shows an example for the **VC-12 Near-end PM** page.

Continue with the steps that follow to display historical PM data for both 15-minute and 24-hour periods.

5. Step 5 Select the **TP Location** for a VC-12 (or a VC-3 or VC-4) TP and click on **Show Interval**.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

VC-12 Near-end PM -- Current 15 minutes

192.168.168.151 > Performance Monitor > VC-12

	TP Location	BBE	ES	SES	UAS	Interval Start Time
●	ST:1/1-1/1/1/2	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/1/3	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/2/1	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/2/2	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/2/3	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/3/1	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/3/2	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/3/3	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/4/1	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/4/2	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/4/3	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/5/1	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/5/2	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/5/3	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/6/1	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/6/2	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/6/3	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/7/1	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/7/2	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/1-1/1/7/3	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/2-1/1/1/2	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/2-1/1/1/3	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/2-1/1/2/1	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/2-1/1/2/2	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/2-1/1/2/3	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/2-1/1/3/1	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/2-1/1/3/2	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)
○	ST:1/2-1/1/3/3	0	0	0	0	Fri May 11 2007 02:45:00 GMT-0700 (Pacific Daylight Time)

Figure 46. Displaying Current VC-12 PM Data

To clear the current PM data for a VC-12 TP, see Figure 46 and follow these steps:

1. On the **VC-12 Near-end PM** page, select one of the STM-1 port entries and use the **Clear Counter Options...** scroll-down button to select one of the available options for clearing the current 15 minute or 24 hour counters, or both.

Monitoring Pointer Justification Counts

The system supports the collection of PM data for pointer justification counts (PJC). Separate counters are provided for detection and generation of both positive and negative pointer adjustments, as shown in Table 38.

Table 38. PJC PM Parameters

PM Parameter	Abbreviation	Description
PPJC-det	Pdet	Positive PJC–detection
PPJC -gen	Pgen	Positive PJC–generation
NPJC-det	Ndet	Negative PJC–detection
NPJC-gen	Ngen	Negative PJC–generation

The system provides only one set of PJC counters for a given AU or TU level:

- One set for AU-4 pointers
- One set for TU-3 or TU-12 pointers

You can indicate the AU-4, TU-3 or TU-12 entity that you wish to monitor.

To display current and historical PM data for selected PJC counters, see Figure 47 on page 102and follow these steps:

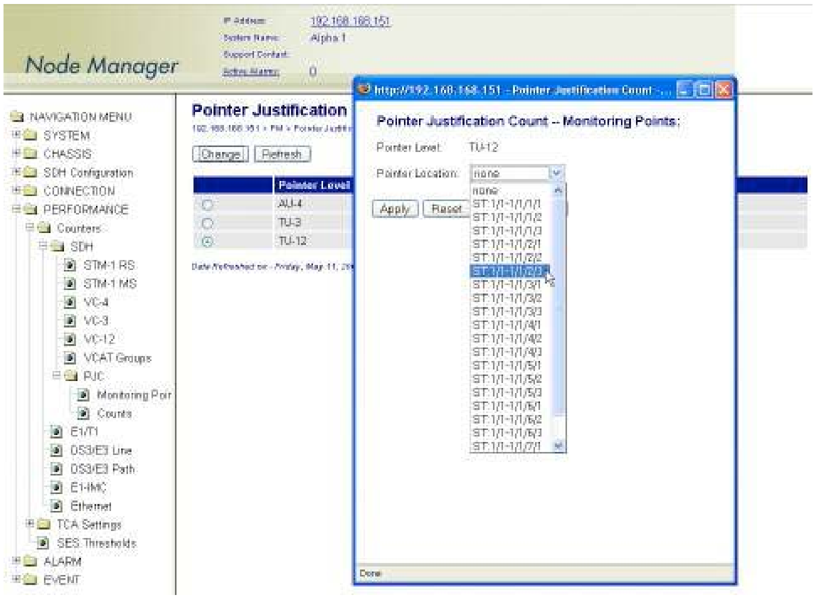
1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select **Counters**.
3. From the expanded **Counters** folder, select **SDH**.
4. From the expanded **SDH** folder, select **PJC**.
5. From the expanded **PJC** folder, select **Monitoring Points**.
6. On the **Pointer Justification Count -- Monitoring Points** page, select one of the **Pointer Level** options (**AU-4, TU-3** or **TU-12**).

At this point, the table on the **Pointer Justification Count -- Monitoring Points** page displays the pointer locations that are currently being monitored, if any were previously selected.

Note By default, no AU or TU pointer locations are monitored.

7. In the **Pointer Justification Count -- Monitoring Points** window, select one of the available Pointer Locations using the scroll-down button.
8. Click on **Apply** and then on **Close** to close the window.

At this point, the table on the **Pointer Justification Counts -- Monitoring Points** page shows the selected AU or TU pointer location. The system starts collecting PM data from this moment.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Pointer Justification

192.168.168.151 > PM > Pointer Justific

	Pointer Level
○	AU-4
○	TU-3
●	TU-12

Date Refreshed on - Friday, May 11, 20

http://192.168.168.151 - Pointer Justification Count - ...

Pointer Justification Count -- Monitoring Points:

Pointer Level: TU-12

Pointer Location: none

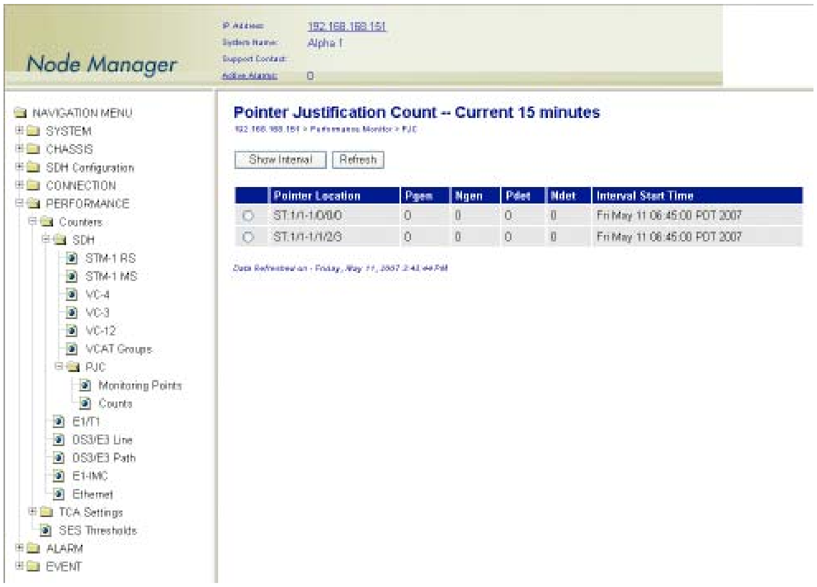
none
ST:1/1-1/1/1/1
ST:1/1-1/1/1/2
ST:1/1-1/1/1/3
ST:1/1-1/1/2/1
ST:1/1-1/1/2/2
ST:1/1-1/1/2/3
ST:1/1-1/1/3/1
ST:1/1-1/1/3/2
ST:1/1-1/1/3/3
ST:1/1-1/1/4/1
ST:1/1-1/1/4/2
ST:1/1-1/1/4/3
ST:1/1-1/1/5/1
ST:1/1-1/1/5/2
ST:1/1-1/1/5/3
ST:1/1-1/1/6/1
ST:1/1-1/1/6/2
ST:1/1-1/1/6/3
ST:1/1-1/1/7/1

Figure 47. Selecting Pointer Locations for PJC Monitoring

9. On the Pointer Justification Counts – Monitoring Points page, select the one of the AU-4, TU- 3 or TU-12 pointer locations.

10. From the expanded PJC folder, select Counts.

At this point, the system displays the PJC count for the current 15-minute period for the selected pointer location. Click on Show Interval to display historical PM data for the 15-minute and 24-hour counters (Figure 48).



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Pointer Justification Count -- Current 15 minutes

192.168.168.151 > Performance Monitor > PJC

	Pointer Location	Pgen	Ngen	Pdet	Ndet	Interval Start Time
○	ST:1/1-1/0/0/0	0	0	0	0	Fri May 11 06:45:00 PDT 2007
○	ST:1/1-1/1/2/3	0	0	0	0	Fri May 11 06:45:00 PDT 2007

Data Refreshed on - Friday, May 11, 2007 2:43:44 PM

Figure 48. Displaying PM Data for PJC Counts

Configuring SDH Threshold Crossing Alerts (TCA)

The system supports threshold registers for SDH performance monitoring parameters. A threshold crossing alert (TCA) event is generated when a monitored event reaches or crosses the preset threshold value within a given measurement period (15 minutes or 24 hours).

To configure the system for reporting TCA events for SDH entities, follow these steps:

Note By default, the reporting of TCA events for SDH entities is disabled.

1. Select the **EVENT** folder from the navigation menu.
2. From the expanded **EVENT** folder, select **Enable TCA Event**.
3. On the **TCA Event Disable / Enable** page, change **TCA Events (layer)** to **On**. The layer can be **RS** or **MS** for STM-1, **HP** for VC-4 or **LP** for both VC-3 and VC-12.
4. Click on **Apply** to complete this task.

Note This is a global setting. For example, enabling the report of TCA events for the LP layer applies to all VC-3 and VC-12 within the system.

To configure the default TCA settings for SDH entities, follow these steps:

1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select the **TCA Settings** folder.
3. From the expanded **TCA Settings** folder, select the required ***SDH entity*** folder. The available ***SDH entity*** options are **STM-1 RS, STM-1 MS, VC-4, VC-3, VC-12** and **PJC**.
4. From the expanded ***SDH entity*** folder, select **Default**.
5. On the ***SDH entity*** **Default TCA Settings** page, select the table entry and click on **Change**.
6. In the ***SDH entity*** **Default TCA Settings** window, change the default TCA settings as required.

Note The system displays the factory default TCA settings when you first open this page. Afterwards, the system displays any recent configuration changes. The preferred method of restoring the original settings is to reenter the values manually.

7. Click on **Apply** and then on **Close** to close the SDH entity Default TCA Settings window.

Note This is a global setting. For example, the VC-12 default values apply to all VC-12 within the system.

To assign custom TCA values for individual SDH entities on the system, continue with Step 8; otherwise, Step 7 completes this task.

8. From the expanded ***SDH entity*** folder, select **Custom**.

At this point, the ***SDH entity* TCA Settings** page displays the current TCA settings for each entity on the system. The table entry indicates Default if the default TCA value is in use for a given parameter or **Custom** (**value**) if the system uses any custom value other than the default.

9. On the ***SDH entity* TCA Settings** page, select the entity that you wish to configure and click on **Change**.

10. In the ***SDH entity* TCA Settings** window, select **Custom** for the TCA settings that you wish to customize and change the setting to any value within the allowable range. You may change the TCA settings for more than one parameter at a time.

11. Click on **Apply** and then on **Close** to close the SDH entity TCA Settings window.

At this point, the ***SDH entity* TCA Settings** page reflects any recent configuration changes.

If you wish to change a TCA setting back to its default setting, select **Default** instead of **Custom** in Step 10.

Displaying the SDH TCA Event Log

To display TCA events for SDH entities, follow these steps:

1. Select the **EVENT** folder from the navigation menu.

2. From the expanded **EVENT** folder, select **Show Event Log**.

At this point, the **Event Log** page displays a list of the 50 most recent TCA event messages. The system keeps up to 500 entries in the event log.

Note The event log is a FIFO (first-in fist-out) log.

Click on **Last 50 Log Entries** or **Next 50 Log Entries** to move around and display the entire contents of the log. Click on **Clear Log** if you wish to delete permanently the current log entries.

SDH Testing

The following section provides the procedures for enabling and disabling loopback tests for STM-1 ports. It also provides the procedures for configuring the STM-1 port to insert errors at the RS and MS layers for testing purposes. The section concludes with the procedures for enabling and disabling the STM-1 scrambler function. The system supports STM-1 Facility Loopback, as shown in Figure 49.

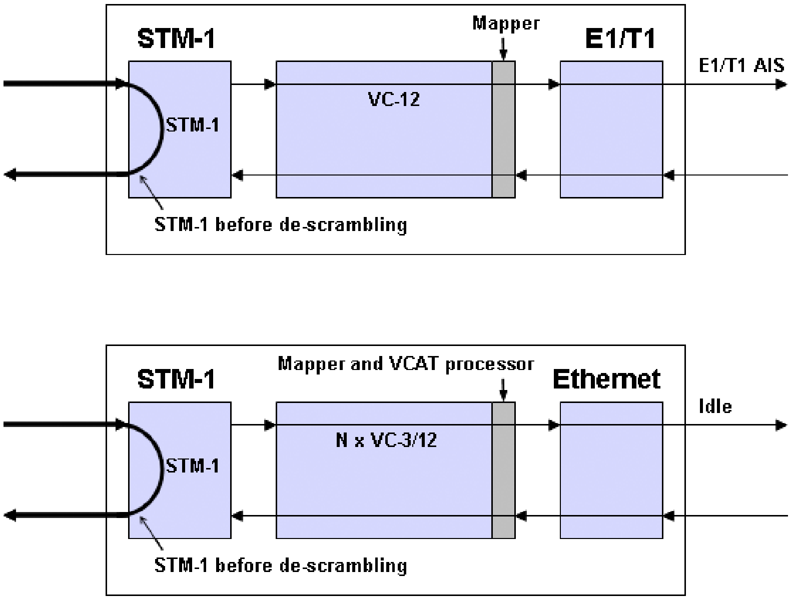

STM-1
Mapper
E1/T1
E1/T1 AIS
VC-12
STM-1
STM-1 before de-scrambling
STM-1
Mapper and VCAT processor
Ethernet
Idle
N x VC-3/12
STM-1
STM-1 before de-scrambling

Figure 49. STM-1 Facility Loopback

Note When STM-1 Facility Loopback is active, the system generates AIS on all E1/T1 and DS3/E3 ports connected to VC-12 and VC-3 termination points and an Idle signal on all Ethernet ports connected to Virtual Concatenation Groups (VCGs)

- STM-1 Terminal Loopback is not supported.

Configuring STM-1 Facility Loopback

To start an STM-1 Facility Loopback test, see Figure 50 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the STM-1 port being tested and click on **Properties**.
4. In the **Port Properties** window, click on **Start Facility Loopback**.

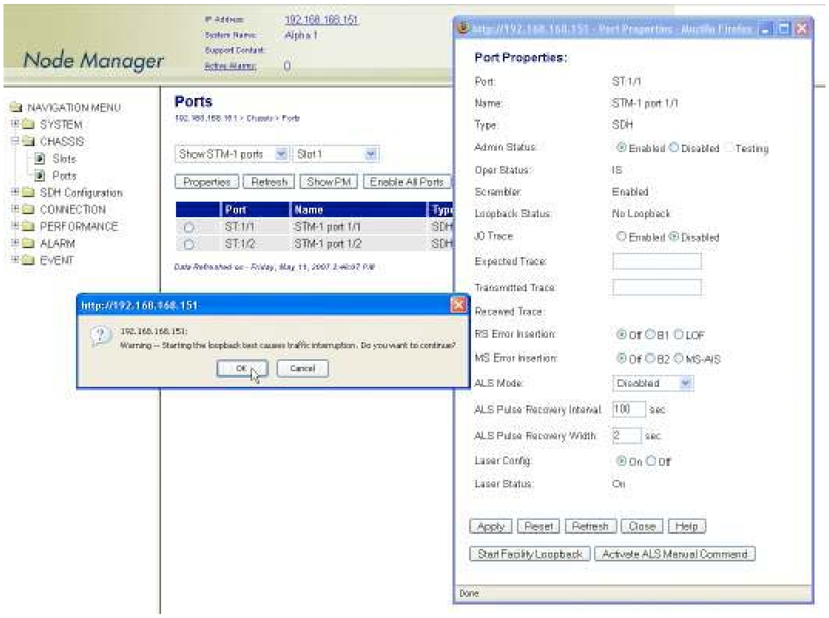
A warning window opens to alert you to the start of the loopback test. Click on **OK** to continue or **Cancel** to cancel the request.

WARNING

Starting an STM-1 Facility Loopback causes traffic disruption for all E1/T1, DS3/E3, or Ethernet client signals connected to VC-3 or VC-12 termination points.

Loopback Status on the **Port Properties** window changes to **Facility Loopback Active**. **Admin Status** for the port changes to **Testing**.

5. Close the window.



Ports

192.168.168.151 > Chassis > Ports

	Port	Name	Type
○	ST 1/1	STM-1 port 1/1	SDH
○	ST 1/2	STM-1 port 1/2	SDH

Data Refreshed on - Friday, May 11, 2007 3:40:57 PM

http://192.168.168.151

192.168.168.151:

Warning -- Starting the loopback test causes traffic interruption. Do you want to continue?

http://192.168.168.151 - Port Properties - Mozilla Firefox

Port Properties:

Port:	ST 1/1
Name:	STM-1 port 1/1
Type:	SDH
Admin Status:	● Enabled ○ Disabled □ Testing
Oper Status:	IS
Scrambler:	Enabled
Loopback Status:	No Loopback
J0 Trace:	○ Enabled ● Disabled
Expected Trace:	
Transmitted Trace:	
Received Trace:	
RS Error Insertion:	● Off ○ B1 ○ LOF
MS Error Insertion:	● Off ○ B2 ○ MS-AIS
ALS Mode:	Disabled
ALS Pulse Recovery Interval:	100 sec
ALS Pulse Recovery Width:	2 sec
Laser Config:	● On ○ Off
Laser Status:	On

Figure 50. Activating STM-1 Facility Loopback

To stop an STM-1 Loopback test, see Figure 50 and follow these steps:

1. In the **Port Properties** window, set **Admin Status** to **Enabled** or **Disabled**, if required.
2. Click on **Apply**.

At this point, **Loopback Status** changes to **No Loopback**. The system resumes any connection previously present between the STM-1 port TU time slots and the E1/T1, DS3/E3, or Ethernet client ports.

3. Close the window.

Configuring Error Insertion

The system allows the insertion of errors and alarm conditions at the STM-1 RS and MS layers for testing purposes. To insert errors at the STM-1 RS layer, see Figure 51and follow these steps:

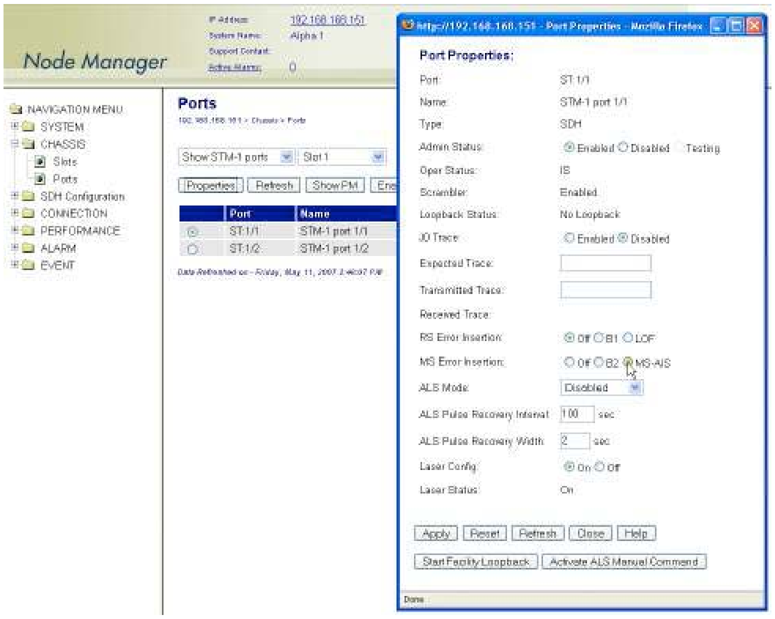
1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the STM-1 port being tested and click on **Properties**.
4. In the **Port Properties** window, select one of the **RS Error Insertion** options (B1 or LOF).
5. Click on **Apply** and then on **Close** to close the window.

When B1 is selected, the system inserts B1 BIP-8 errors on every STM-1 frame until the RS Error Insertion is changed to Off. When LOF is selected, the system inserts errors on the A1 A2 framing bytes on every STM-1 frame until the RS Error Insertion is changed to Off. Activating the LOF option, causes LOF detection at the far-end equipment connected to the OS-10.

To insert errors at the STM-1 MS layer, see Figure 51and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the STM-1 port being tested and click on **Properties**.
4. In the **Port Properties** window, select one of the **MS Error Insertion** options (B2 or MS-AIS)
5. Click on **Apply** and then on **Close** to close the window.

When B2 is selected, the system inserts B2 BIP-24 errors on every STM-1 frame until the MS Error Insertion is changed to Off. When MS-AIS is selected, the system inserts MS-AIS until the MS Error Insertion is changed to Off.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Ports

192.168.168.151 > Chassis > Ports

	Port	Name
●	ST:1/1	STM-1 port 1/1
○	ST:1/2	STM-1 port 1/2

Data Refreshed on - Friday, May 11, 2007 2:46:07 PM

http://192.168.168.151 - Port Properties - Mozilla Firefox

Port Properties:

Port: ST 1/1
Name: STM-1 port 1/1
Type: SDH
Admin Status: ● Enabled ○ Disabled Testing
Oper Status: IS
Scrambler: Enabled
Loopback Status: No Loopback
J0 Trace: ○ Enabled ● Disabled
Expected Trace:
Transmitted Trace:
Received Trace:
RS Error Insertion: ● Off ○ B1 ○ LOF
MS Error Insertion: ○ Off ○ B2 ● MS-AIS
ALS Mode: Disabled
ALS Pulse Recovery Interval: 100 sec
ALS Pulse Recovery Width: 2 sec
Laser Config: ● On ○ Off
Laser Status: On

Figure 51. Inserting STM-1 Errors

Virtual Concatenation (VCAT)

The system supports the connection of Ethernet traffic over SDH using virtual concatenation (VCAT) groups, in accordance with ITU-T Recommendation G.707. The following section provides the procedures for provisioning and monitoring virtual VCAT groups (VCGs).

NOTE: You must create a VCG before connecting Ethernet ports to the STM-1 port.

Introduction to VCAT

VCAT groups are flexible TDM payload channels for Ethernet traffic. The standard notation for a VCG is VC-n-Xv, where “VC-n” is the capacity of the constituent members, and “X” is the number of members. The letter “v” indicates that the “X” members form a virtual concatenation group. The total capacity of the VC-n-Xv is thus X * VC-n. A VC-3-2v supports a full-rate Fast Ethernet service at 100 Mbit/s. A VCG with a single VC-3 member (that is, a VC-3-1v) supports the transport of fractional Fast Ethernet services at 50 Mbit/s.

For finer bandwidth provisioning, the size of a VC-12-Xv can be adjusted in 2-Mbit/s increments up to the required bandwidth. A VC-12-5v, for instance, supports a full-rate Ethernet 10BASE-T service at 10 Mbit/s. A VC-12-50v supports a full-rate Fast Ethernet service at 100 Mbit/s.

VCAT Group Features for the OS1052

The OS1052 base system contains two Ethernet ports and supports the creation of up to 2 VCGs at the VC-3 and VC-12 levels (one VCG for each port). The two VCGs can be combined in various ways. Table 39 provides the provisioning rules for the creation of VCGs on the OS1052 base system (slot 1).

Table 39. VCG Provisioning Rules for OS1052 Base System (Slot 1)

VCG Combination	Group 1	Group 2	Restrictions
1	VC-3-1v	VC-3-1v	None
2	VC-3-1v	VC-12-Xv	X = 1 to 12
3	VC-3-2v	VC-3-1v	None
4	VC-3-2v	VC-12-Xv	X = 1 to 12
5	VC-12-Xv	VC-12-Yv	X + Y should be less than or equal to 16, while X or Y does not exceed 12

The OS1052 supports additional VCGs through the use of the high-density Ethernet (HD-ENET) expansion module. In contrast to the Ethernet ports on the base system, the HD-ENET module provides full flexibility in the creation of VCGs for slots 2 and 3. The module provides full access to all the available TU-12 and TU-3 time slots in the system.

The HD-ENET module supports two configuration modes: VCG 16 and VCG 8. In VCG 16 mode, you can create up to 16 VCGs using the available time slots. In this mode, the maximum size of a VCG group is limited to 18 VC-12 members. Use this mode when you require provisioning of a large number of Ethernet services with with reduced bandwidth requirements. In VCG 8 mode, you can create up to 8 VCGs with a maximum of 50 VC-12 members.

The maximum number of VCGs depends on the number of available time slots on the STM-1 and size of the existing VCGs. For example, if the STM-1 is configured with 63 TU-12 time slots (and assuming that none of the time slots is currently in use), the module can support 16 VCGs: 15 VC-12-4v and one VC-12-1v. On the other hand, if you configure a large VCG, such as a VC-12-60v, only three time slots remain for a single VC-

12-3v or 3 VC-12-1v. Any combination of VCG size and number is possible, as long as the total number of VC-3 and VC-12 paths in all VCGs in a module do not exceed the available number of time slots.

The system rejects any attempt to create VCGs that do not meet these provisioning rules.

VCAT Group Features for the OS1063

The OS1063 does not contain Ethernet ports in slot 1 (the base system). Therefore, the OS1063 supports VCGs only through the use of the high-density Ethernet (HD-ENET) expansion module in slots 2 and 3.

Summary of VCAT Group Features for the OS-10-Series Systems

Table 40 provides a summary of the VCAT features for the OS1052 using slots 1-3 (base and expansion slots) and for the OS1063 using slots 2-3 (expansion slots only).

Table 40. Summary of VCAT Features for the OS-10-Series

Slot ID	Slot Type	Maximum No. of VCGs	VC-3-Xv		VC-12-Xv	
			Provisioning Range	Bandwidth (Mbit/s)	Provisioning Range	Bandwidth (Mbit/s)
1	Base (OS1052 only)	2	X = 1 to 2	48.96 to 97.92	X = 1 to 12	2.176 to 26.112
2 or 3	Expansion (HD-ENET)	8	X = 1 to 2	48.96 to 97.92	X = 1 to 50	2.176 to 108.8
		16	X = 1 to 2	48.96 to 97.92	X = 1 to 18	2.176 to 39.168

Note VCG support in slots 2 and 3 requires the use of the high-density Ethernet (HD-ENET) module. See chapter 13 for details about the installation and operation of this module.

GFP Packet Transport Considerations

The system removes the inter-packet gaps (IPG) between incoming Ethernet frames before encapsulating the frames into a VCG using generic framing procedure (GFP). This removal of the IPG results in more efficient use of the VCG capacity. The system reinserts the IPG for outgoing frames sent over the Ethernet ports.

When the average rate of the incoming Ethernet port traffic exceeds the allocated VCG capacity, it causes an internal buffer overflow condition with a resulting drop in packets. This overflow condition results in the generation of an Ethernet Buffer Overflow alarm. The system buffers, however, provide sufficient capacity to absorb short-term bursts above the allocated capacity.

Note If packet congestion occurs, flow control at the Ethernet and TCP levels automatically reduce the incoming packet rate to match the provisioned TDM channel bandwidth.

VCG Notation

The system uses the following notation to identify VCGs. VCG:slot-number. For example, VCG:3-10 refers to the tenth VCG on slot 3.

Note You can connect only Ethernet traffic between ports and VCGs that reside on the same slot. For example, only the Ethernet ports on slot 2 have access to the VCGs that you create on that slot.

Differential Delay

Because VCG members may travel through separate VC-n connection paths across the SDH network, it is possible for individual members to arrive at the far end of the VCG connection with different delays relative to each other. These delays are compensated using internal "differential delay" buffers. These buffers realign the incoming VCG members to a common phase prior to extracting the Ethernet traffic from the combined payload capacity.

Table 41 provides the maximum differential delay that the system can compensate for different types of ports. The system generates a loss of alignment (LOA) alarm if the VCAT processor cannot reconstruct the VCG because the VCG members exceed the differential delay allocation for the system.

Table 41. Differential Delay Support

Ethernet Ports on the . . .	Maximum Differential Delay
Base system	±256 msec
HD-ENET module	±128 msec

Note This differential delay allocation allows the transport of Ethernet signals between two OS-10 nodes using transcontinental and transoceanic links.

Creating a VCG

This section provides the procedures for the creation of VCGs at the VC-3 and VC-12 levels.

To create a VCG at the VC-3 level, see Figure 52 on page 113 and follow these steps:

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select **VCAT Groups**.
3. On the **VCAT Groups** page, click on **Create VCAT Group**.
4. Select the slot in which you want to create the VCG using the **Slot** scroll-down button.

Note The system displays the entries for slots 2 and 3 only when these slots are provisioned with the HD-ENET module.

- The system assigns a unique VCG ID for the slot after creation of the VCG. This ID is indicated in the **VCG ID** field. The VCG ID contains the slot number and VCG number for that slot. The notation for the VCG ID is as follows: VCG:slot-number.

- As an option, you may choose to identify the newly created VCG with a name. Type the VCG name in the Name field or leave it blank.

5. Set the **VCG mode** for the HD-ENET module, if present in slot 2 or 3.

Note The system only allows setting the VCG mode when the HD-ENET module contains no VCGs. Setting the VCG mode is not applicable for the base system ports in slot 1.

6. To enable the LCAS function for the VCG, set **LCAS** to **Enabled**. Otherwise, continue with Step 7.

Note The system supports the enabling of the LCAS function only in slots 2 and 3, when the slots contain the HD-ENET module.

CAUTION Make sure that the HD-ENET modules in your OS-10 system support the required firmware revision for the use of the LCAS function.

With the LCAS function enabled, you may configure the LCAS Hold-Off Time and the LCAS WTR Time to different values other than the default value of 0.

The LCAS Hold-Off time is the amount of time the LCAS processor waits before the temporary removal of a member from the VCG after reception of an MST (Sk) = FAIL for that member. The LCAS processor removes the member from the VCG only if the member remains in the failed condition at the time the hold-off time expires. The timer is set in multiples of 100 msec, from 0 to 10 sec (0 sec as default).

The LCAS WTR (wait-to-restore) time is the amount of time the LCAS processor waits before the system reinserts a failed member back into a VCG after the MST (Sk) for that member changes from FAIL back to OK. The provisioning range for the LCAS WTR time is 0 to 12 minutes, and is set in 1 minute increments (0 minutes as default).

7. In the **Create VCAT Group** window, set **Level** to **VC-3** to create a VC-3-Xv.
8. In the **Create VCAT Group** window, select the No. of Members for the new VCG using the scroll-down button.

At this point, the system provides a list of available TU-3 time slots in the STM-1 using the SDH indexing scheme.

Note When the system is configured for Linear 1+1 MSP or SNCP operation, the list includes only the TU-3 time slots for STM-1 port 1 (ST:1/1). However, when both ports are unprotected, the list includes the available time slots for both ports (ST:1/1 and ST:1.2).

9. In the **Create VCAT Group** window, select the TU-3 **Member Locations** for each VCG member.

The system highlights default member locations according to the number of VCG members that you select. You may, however, choose TU-3 time slots other than the default locations.

To select more than one member from the list, click on individual entries while pressing the Ctrl key. (The system highlights any entry that you select from the list. You can select any entry from the list, whether the member locations are contiguous or not.)

Note To select a range of consecutive entries from the list, select the first entry and then select the last entry while pressing the Shift key.

- Use the **Reset** button to restore the window to the default member location.

- Make sure that the number of selected entries from the list matches the No. of Members before proceeding with Step 8; otherwise, the system rejects the creation of the VCG.

10. Click on **Apply** to initiate the creation of the VCG.

CAUTION

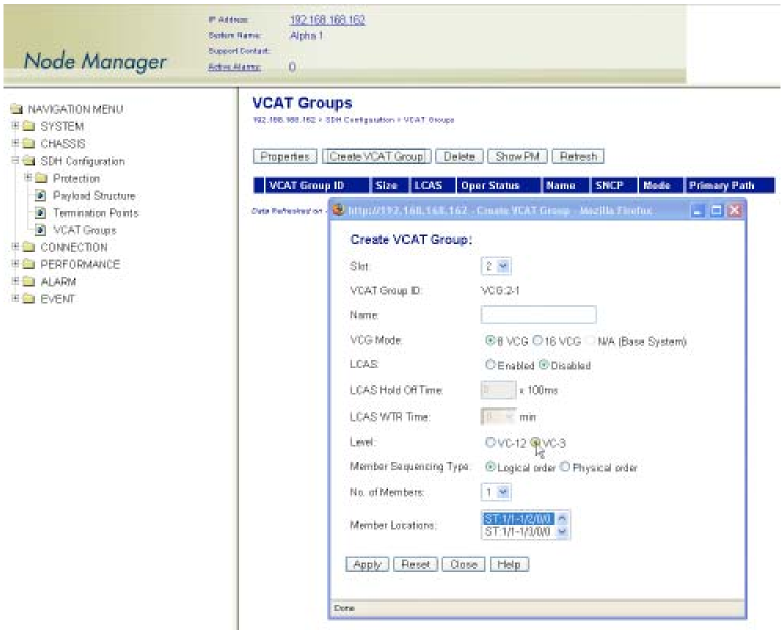
The **Create VCAT Group** window closes automatically after the system completes the creation of the VCG. For VCGs with a large number of members, the system may take a few seconds to create the VCG and close the window. Closing the window manually before.the process is complete may cause an error or partial creation of the new VCG (that is, the new VCG contains a reduced number of members.)

At this point, the **VCAT Groups** page displays all current VCAT groups in the system, including the newly created VCG. The table contains a separate entry for each provisioned VCG. Each entry contains a summary of the VCG properties, including the VCAT Group ID, VCG Size, and Name. The table entry also contains the Admin Status and Oper Status of the VCG and whether or not SNCP protection is enabled or disabled. The SNCP Mode and Primary Path for the VCG are also displayed.

Note The **VCG Admin Status** changes from **Disabled** to **Enabled** when you connect an Ethernet port to the VCG.

- The **Oper Status** indicates that the VCG is IS (in service) when the Admin Status is Enabled and no VCG alarms are present. Otherwise, the Oper Status indicates OOS (out of service).

- When you create a VCG at VC-3 level, the system reserves the TU-3 time slots that you assign for each VCG member. You cannot use these time slots to create another VCG unless you delete the first VCG. Each TU-3 sends the unequipped signal until the moment that you create a connection between an Ethernet port and the VCG. (Refer to §11.3 for details.) At that point, the system equips each VC-3 for carrying GFP payload.



Create VCAT Group:

Slot: 2

VCAT Group ID: VCG:2-1

Name:

VCG Mode: ● 8 VCG ○ 16 VCG ○ N/A (Base System)

LCAS: ○ Enabled ● Disabled

LCAS Hold Off Time: 0 x 100ms

LCAS WTR Time: 0 min

Level: ○ VC-12 ● VC-3

Member Sequencing Type: ● Logical order ○ Physical order

No. of Members: 1

Member Locations: ST:1/1-1/2/0/0
ST:1/1-1/3/0/0

Figure 52. Provisioning a VCG at the VC-3 Level

To configure the SNCP settings of a VCG, see Figure 53 on page 114 and follow these steps:

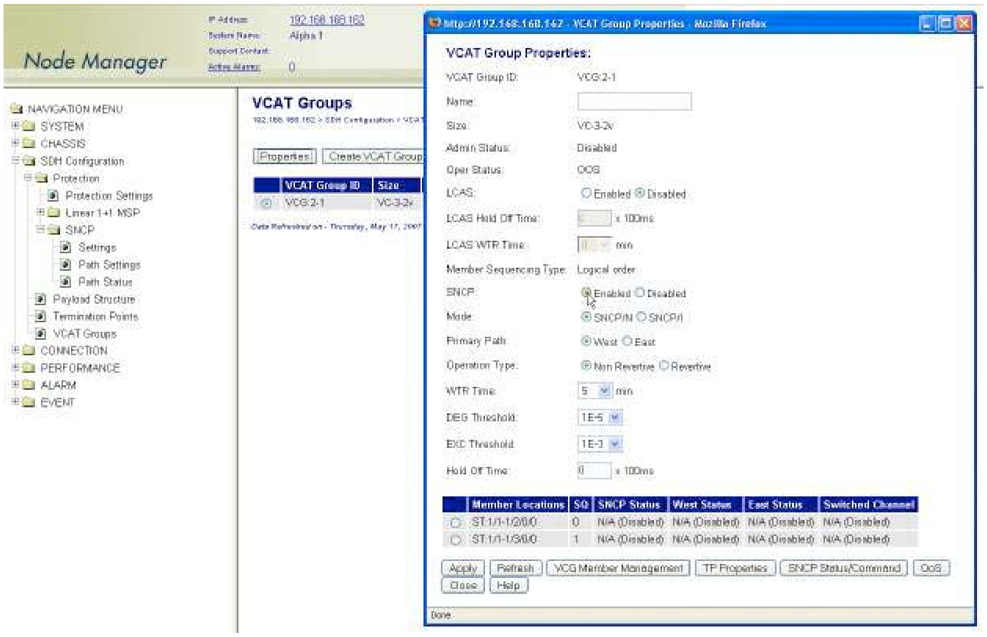
1. On the **VCAT Groups** page, select the table entry containing the required VCG and click on **Properties**.

At this point, if the VCG is connected to an STM-1 port pair that is configured for operation in SNCP mode, the **VCAT Group Properties** window contains the SNCP path properties for the VCG. You can set the SNCP path properties in accordance with the descriptions in Table 54.

2. In the **VCAT Group Properties** window, set **SNCP** to **Enabled**.

Note The SNCP path properties for the VCG apply to all members of the VCG. The system ensures that the SNCP path properties of all VCG members remain the same.

The **VCAT Group Properties** window also contains the SNCP path status for all the VCG members (see Table 55 for a description of the table fields and entries). To activate any of the external commands for SNCP path switching for an individual VCG member, select the table entry for the member and click on **SNCP Status/Command**.



	VCAT Group ID	Size
●	VCG:2-1	VC-3-2v

VCAT Group Properties:

VCAT Group ID: VCG:2-1

Name:

Size: VC-3-2v

Admin Status: Disabled

Oper Status: OOS

LCAS: ○ Enabled ● Disabled

LCAS Hold Off Time: x 100ms

LCAS WTR Time: min

Member Sequencing Type: Logical order

SNCP: ● Enabled ○ Disabled

Mode: ● SNCP/N ○ SNCP/I

Primary Path: ● West ○ East

Operation Type: ● Non Revertive ○ Revertive

WTR Time: 5 min

DEG Threshold: 1E-5

EXC Threshold: 1E-3

Hold Off Time: 0 x 100ms

	Member Locations	SQ	SNCP Status	West Status	East Status	Switched Channel
○	ST:1/1-1/2/0/0	0	N/A (Disabled)	N/A (Disabled)	N/A (Disabled)	N/A (Disabled)
○	ST:1/1-1/3/0/0	1	N/A (Disabled)	N/A (Disabled)	N/A (Disabled)	N/A (Disabled)

Figure 53. Configuring the SNCP Settings of a VCG at the VC-3 Level

To view and configure the properties of a VCG member, see Figure 54 on page 115 and follow these steps:

1. On the **VCAT Groups** page, select the table entry containing the required VCG and click on **Properties**.
2. In the **VCAT Group Properties** window, select one of the VCG members and click on **TP Properties**.

At this point, the system displays the current VC-3 TP settings for the selected VCG member.

To configure the J1 trace message on the VC-3, continue with Step 3.

Note To configure the TP properties of a VCG member, the VCG must be connected to an Ethernet port .

3. In the **TP Properties** window, set the **J1 Trace** to **Enabled**.
   – Set **TIM Monitor** to **Enabled**, if you wish to detect trace identifier mismatch (TIM) defects for the VC-3 TP using the J1 trace.
   – Set **TIM Action** to **Enabled**, if you wish to generate a consequent action (AIS downstream and LP-RDI upstream) upon detection of a TIM defect for the VC-3 TP using the J1 trace.
4. Type the **Expected Trace** and the **Transmitted Trace** using up to 15 ASCII characters for each field.

Note The system inserts the transmitted trace into the outgoing J1 byte for the VC-3 TP. The system does not allow enabling the J1 trace with the expected trace and transmitted trace fields empty. The system displays the **Received Trace** message if any is being received from the incoming J1 byte for this VC-3 TP.

To configure the error insertion features for the TP, continue with Step 5; otherwise, go directly to Step 6 to complete this task.

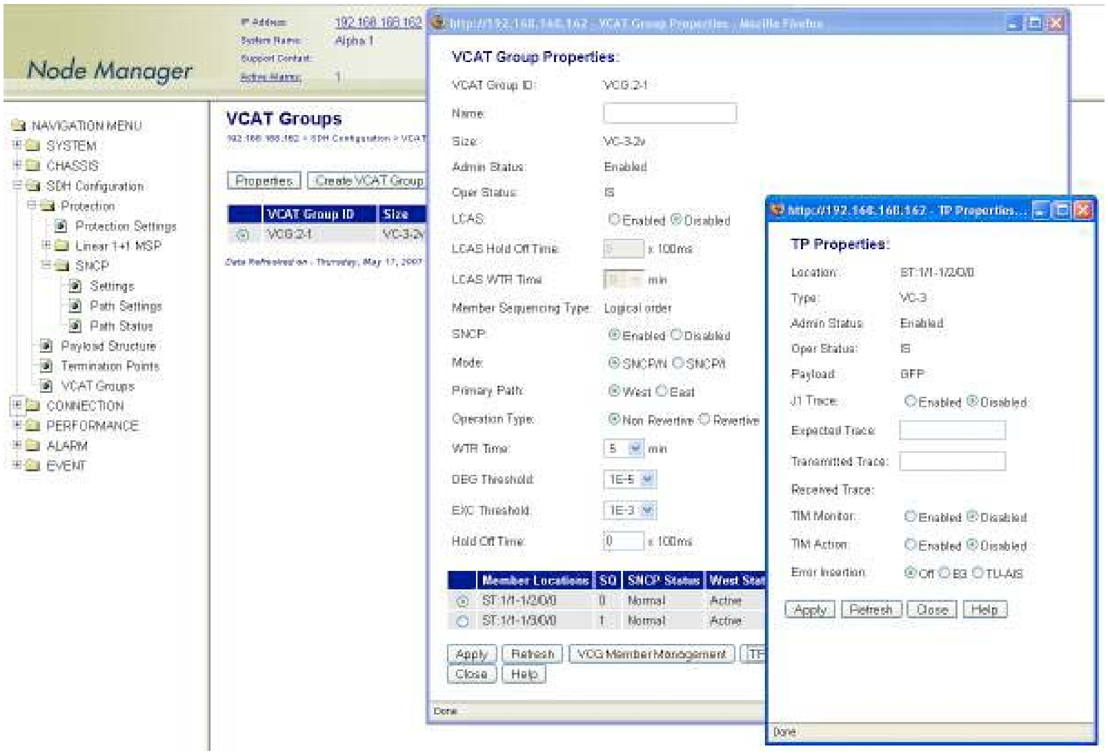
5. In the **TP Properties** window, select one of the **Error Insertion** options (**B3** or **TU-AIS**).

> **Note** When B3 is selected, the system inserts B3 BIP-8 errors on every frame of the VC-3 TP until the Error Insertion is changed to Off.

> **Note** When TU-AIS is selected, the system inserts TU-AIS on the TU-3 until the Error Insertion is changed to Off. Activating the TU-AIS option causes TU-AIS detection at the farend equipment connected to the OS-10 system.

6. Click on **Apply** and then on **Close** to close the TP Properties window.

7. Click on **Close** to close the VCAT Group Properties window.



	VCAT Group ID	Size
●	VCG:2-1	VC-3-2v

VCAT Group Properties:

VCAT Group ID: VCG:2-1
Name:
Size: VC-3-2v
Admin Status: Enabled
Oper Status: IS
LCAS: ○Enabled ●Disabled
LCAS Hold Off Time: 0 x 100ms
LCAS WTR Time: 0 min
Member Sequencing Type: Logical order
SNCP: ●Enabled ○Disabled
Mode: ●SNCP/N ○SNCP/I
Primary Path: ●West ○East
Operation Type: ●Non Revertive ○Revertive
WTR Time: 5 min
DEG Threshold: 1E-5
EXC Threshold: 1E-3
Hold Off Time: 0 x 100ms

	Member Locations	SQ	SNCP Status	West Stat
●	ST:1/1-1/2/0/0	0	Normal	Active
○	ST:1/1-1/3/0/0	1	Normal	Active

TP Properties:

Location: ST:1/1-1/2/0/0
Type: VC-3
Admin Status: Enabled
Oper Status: IS
Payload: GFP
J1 Trace: ○Enabled ●Disabled
Expected Trace:
Transmitted Trace:
Received Trace:
TIM Monitor: ○Enabled ●Disabled
TIM Action: ○Enabled ●Disabled
Error Insertion: ●Off ○B3 ○TU-AIS

Figure 54. Configuring the Properties of a VC-3 VCG Member

To create a VCG at the VC-12 level, see Figure 55 on page 118 and follow these steps:

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select **VCAT Groups**.
3. On the **VCAT Groups** page, click on **Create VCAT Group**.
4. Select the slot in which you want to create the VCG using the **Slot** scroll-down button.

Note The system displays the entries for slots 2 and 3 only when these slots are provisioned with the HD-ENET module.

- The system assigns a unique VCG ID for the slot after creation of the VCG. This ID is indicated in the **VCG ID** field. The VCG ID contains the slot number and VCG number for that slot. The notation for the VCG ID is as follows: VCG:slot-number.

- As an option, you may choose to identify the newly created VCG with a name. Type the VCG name in the **Name** field or leave it blank.

5. Set the **VCG mod**e for the HD-ENET module, if present in slot 2 or 3.

Note The system only allows setting the VCG mode when the HD-ENET module contains no VCGs. Setting the VCG mode is not applicable for the base system ports in slot 1.

6. To enable the LCAS function for the VCG, set **LCAS** to **Enabled**. Otherwise, continue with Step 7.

Note The system supports the enabling of the LCAS function only in slots 2 and 3, when the slots contain the HD-ENET module.

CAUTION

Make sure that the HD-ENET modules in your OS-10 system support the required firmware revision for the use of the LCAS function.

With the LCAS function enabled, you may configure the **LCAS Hold-Off Time** and the **LCAS WTR Time** to different values other than the default value of 0.

The LCAS Hold-Off time is the amount of time the LCAS processor waits before the temporary removal of a member from the VCG after reception of an MST (Sk) = FAIL for that member. The LCAS processor removes the member from the VCG only if the member remains in the failed condition at the time the hold-off time expires. The timer is set in multiples of 100 msec, from 0 to 10 sec (0 sec as default).

The LCAS WTR (wait-to-restore) time is the amount of time the LCAS processor waits before the system reinserts a failed member back into a VCG after the MST (Sk) for that member changes from FAIL back to OK. The provisioning range for the LCAS WTR time is 0 to 12 minutes, and is set in 1 minute increments (0 minutes as default).

7. In the **Create VCAT Group** window, set **Level** to **VC-12** to create a VC-12-Xv.

8. In the **Create VCAT Group** window, select the **No. of Members** for the new VCG using the scroll-down button.

At this point, the system provides a list of available TU-12 timeslots in the STM-1 using the SDH indexing scheme. By default, the system displays the TU-12 timeslots in logical sequence order. To display the timeslots in physical order, set the **Member Sequencing Type** to **Physical order**.

Note With the LCAS function disabled, the system assigns the sequence number for VCG members strictly in accordance to the order in which the timeslots appear on the list. For VCG interworking purposes with other equipment, make sure that the member sequencing type is the same for both the OS-10 and the other equipment.

- When the system is configured for Linear 1+1 MSP or SNCP operation, the list includes only the TU-12 time slots for STM-1 port 1 (ST:1/1). However, when both ports are unprotected, the list includes the available time slots for both ports (ST:1/1 and ST:1.2).

9. In the **Create VCAT Group** window, select the **TU-12 Member Locations** for each VCG member.

The system highlights default member locations according to to the number of VCG members that you select. You may, however, choose TU-12 time slots other than the default locations.

To select more than one member from the list, click on individual entries while pressing the Ctrl key. (The system highlights any entry that you select from the list. You can select any entry from the list, whether the member locations are contiguous or not.)

Note To select a range of consecutive entries from the list, select the first entry and then select the last entry while pressing the Shift key.

- Use the **Reset** button to restore the window to the default configuration of five members.

- Make sure that the number of selected entries from the list matches the **No. of Members** before proceeding with Step 8; otherwise, the system rejects the creation of the VCG.

10. Click on **Apply** to initiate the creation of the VCG.

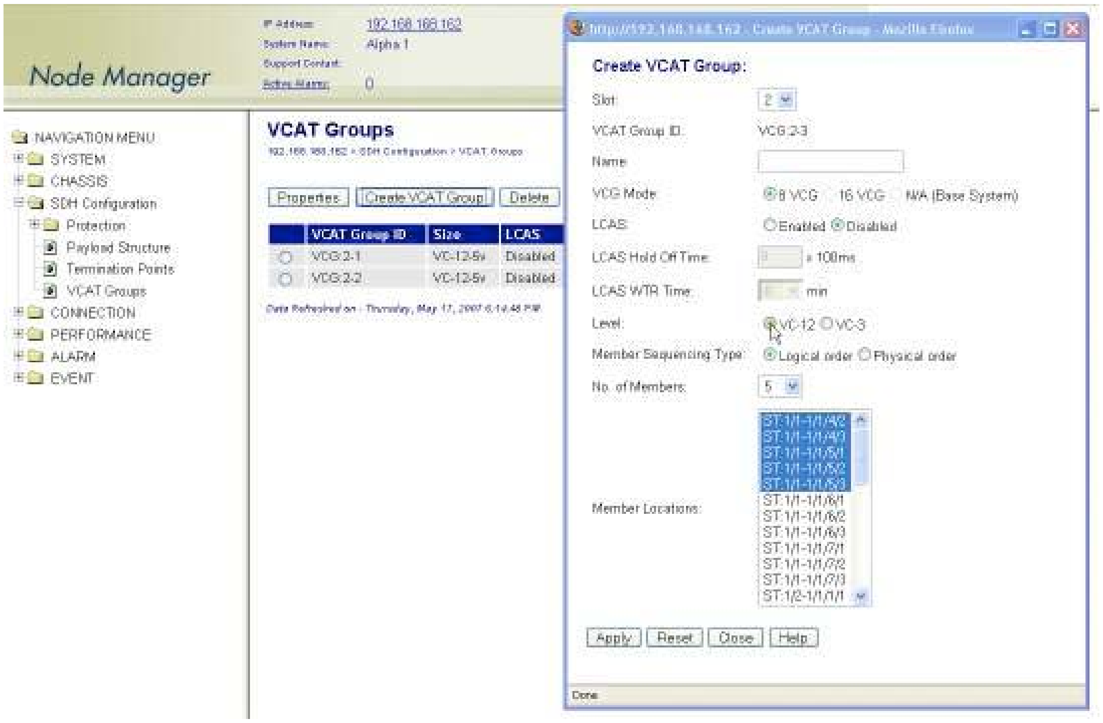
CAUTION

The **Create VCAT Group** window closes automatically after the system completes the creation of the VCG. For VCGs with a large number of members, the system may take a few seconds to create the VCG and close the window. Closing the window manually before.the process is complete may cause an error or partial creation of the new VCG (that is, the new VCG contains a reduced number of members.)

At this point, the VCAT Groups page displays all current VCAT groups in the system, including the newly created VCG. The table contains a separate entry for each provisioned VCG. Each entry contains a summary of the VCG properties, including the VCAT Group ID, VCG Size, and Name. The table entry also contains the Admin Status and Oper Status of the VCG and whether or not SNCP protection is enabled or disabled. The SNCP Mode and Primary Path for the VCG are also displayed.

Note The VCG Admin Status changes from Disabled to Enabled when you connect an Ethernet port to the VCG.

- The Oper Status indicates that the VCG is IS (in service) when the Admin Status is Enabled and no VCG alarms are present. Otherwise, the Oper Status indicates OOS (out of service).
- When you create a VCG at the VC-12 level, the system reserves the TU-12 time slots that you assign for each VCG member. You cannot use these time slots to create another VCG unless you delete the first VCG. Each TU-12 sends the unequipped signal until the moment that you create a connection between an Ethernet port and the VCG. (Refer to §11.3 for details.) At that point, the system equips each VC-12 for carrying a GFP payload.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

VCAT Groups

192.168.168.162 > SDH Configuration > VCAT Groups

	VCAT Group ID	Size	LCAS
○	VCG:2-1	VC-12-5v	Disabled
○	VCG:2-2	VC-12-5v	Disabled

Data Refreshed on : Thursday, May 17, 2007 6:14:48 PM

Create VCAT Group:

Slot: 2
VCAT Group ID: VCG:2-3
Name:
VCG Mode: ● 8 VCG 16 VCG N/A (Base System)
LCAS: ○ Enabled ● Disabled
LCAS Hold Off Time: 0 x 100ms
LCAS WTR Time: min
Level: ● VC-12 ○ VC-3
Member Sequencing Type: ● Logical order ○ Physical order
No. of Members: 5
Member Locations: ST:1/1-1/1/4/2, ST:1/1-1/1/4/3, ST:1/1-1/1/5/1, ST:1/1-1/1/5/2, ST:1/1-1/1/5/3 (selected); ST:1/1-1/1/6/1, ST:1/1-1/1/6/2, ST:1/1-1/1/6/3, ST:1/1-1/1/7/1, ST:1/1-1/1/7/2, ST:1/1-1/1/7/3, ST:1/2-1/1/1/1

Figure 55. Provisioning a VCG at the VC-12 Level

To view and configure the properties of a VC-12 VCG member, see Figure 56 on page 120 and follow these steps:

1. On the **VCAT Groups** page, select the table entry containing the required VCG and click on **Properties**.
2. In the VCAT Group Properties window, select one of the VCG members and click on TP Properties.

At this point, the system displays the current VC-12 TP settings for the selected VCG member.

To configure the J2 trace message on the VC-12, continue with Step 3.

Note To configure the TP properties of a VCG member, the VCG must be connected to an Ethernet port.

3. In the **TP Properties** window, set the **J2 Trace** to **Enabled**.
   - Set **TIM Monitor** to **Enabled**, if you wish to detect trace identifier mismatch (TIM) defects for the VC-12 TP using the J2 trace.
   - Set **TIM Action** to **Enabled**, if you wish to generate a consequent action (AIS downstream and LP-RDI upstream) upon detection of a TIM defect for the VC-12 TP using the J2 trace.
4. Type the **Expected Trace** and **Transmitted Trace** using up to 15 ASCII characters for each field.

Note The system inserts the transmitted trace into the outgoing J2 byte for the VC-12 TP.

- The system does not allow enabling the J2 trace with the expected trace and transmitted trace fields empty.
- The system displays the **Received Trace** if any message is being received from the incoming J2 byte for this VC-12 TP.

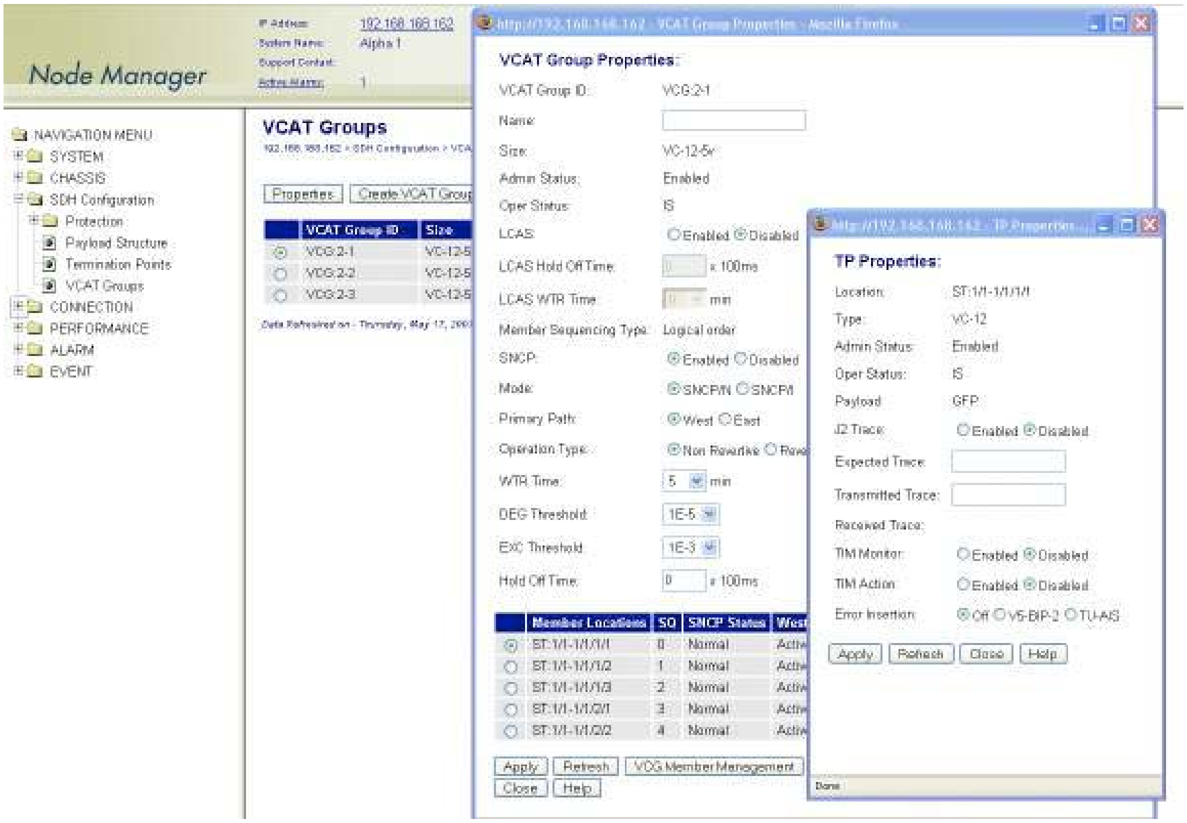
To configure the error insertion features for the TP, continue with Step 5; otherwise, go directly to Step 6 to complete this task.

5. In the **TP Properties** window, select one of the **Error Insertion** options (**V5-BIP-2** or **TU-AIS**).

Note When **V5-BIP-2** is selected, the system inserts V5 BIP-2 errors on every frame of the VC-12 TP until the Error Insertion is changed to Off.

- When **TU-AIS** is selected, the system inserts TU-AIS on the TU-12 until the Error Insertion is changed to Off. Activating the TU-AIS option causes TU-AIS detection at the farend equipment connected to the OS-10.

6. Click on **Apply** and then on **Close** to close the TP Properties window.
7. Click on **Close** to close the VCAT Properties window.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 1

VCAT Groups

192.168.168.162 > SDH Configuration > VCA

	VCAT Group ID	Size
●	VCG:2-1	VC-12-5
○	VCG:2-2	VC-12-5
○	VCG:2-3	VC-12-5

Data Refreshed on - Thursday, May 17, 200

http://192.168.168.162 - VCAT Group Properties - Mozilla Firefox

VCAT Group Properties:

VCAT Group ID:	VCG:2-1
Name:	
Size:	VC-12-5v
Admin Status:	Enabled
Oper Status:	IS
LCAS:	○ Enabled ● Disabled
LCAS Hold Off Time:	0 x 100ms
LCAS WTR Time:	0 min
Member Sequencing Type:	Logical order
SNCP:	● Enabled ○ Disabled
Mode:	● SNCP/N ○ SNCP/I
Primary Path:	● West ○ East
Operation Type:	● Non Revertive ○ Reve
WTR Time:	5 min
DEG Threshold:	1E-5
EXC Threshold:	1E-3
Hold Off Time:	0 x 100ms

	Member Locations	SQ	SNCP Status	West
●	ST:1/1-1/1/1/1	0	Normal	Activ
○	ST:1/1-1/1/1/2	1	Normal	Activ
○	ST:1/1-1/1/1/3	2	Normal	Activ
○	ST:1/1-1/1/2/1	3	Normal	Activ
○	ST:1/1-1/1/2/2	4	Normal	Activ

http://192.168.168.162 - TP Properties

TP Properties:

Location:	ST:1/1-1/1/1/1
Type:	VC-12
Admin Status:	Enabled
Oper Status:	IS
Payload:	GFP
J2 Trace:	○ Enabled ● Disabled
Expected Trace:	
Transmitted Trace:	
Received Trace:	
TIM Monitor:	○ Enabled ● Disabled
TIM Action:	○ Enabled ● Disabled
Error Insertion:	● Off ○ V5-BIP-2 ○ TU-AIS

Figure 56. Configuring the Properties of a VC-12 VCG Member

Removing a VCG

To remove an existing VCG, see Figure 52 on page 113 and follow these steps:

1. Select a VCG on the **VCAT Groups** page.
2. Click on **Delete** to remove the VCG.

At this point, the system removes the VCG and it is no longer displayed in the table.

Note The system automatically disables the VCG after its deletion. All constituent VCG members are also disabled and the system starts sending the unequipped signal over the TU time slots. The time slots are now available for other connections.

- The system displays an error message if you try to delete a VCG that supports an existing Ethernet port connection. You must first remove the connection before deleting the VCG.

Monitoring VCG Alarms

Table 42 provides a list of the VCG alarms that the system supports.

Table 42. VCG Alarms

Alarm	Description	Occurs when the VCAT Processor . . .
LOA	Loss of Alignment	Cannot assemble the concatenated payload because one or more VCG members exceed the differential delay allocation.
LOM	Loss of Multiframe	Loses synchronization from: MFI-1 or MFI-2 for any member of a VC-3-Xv or MFAS or LO-VCAT multiframe for any member of a VC-12-Xv
SQM	Sequence Indicator Mismatch	Receives a sequence number different from the one provisioned for a VCG member.

To display VCG alarms, if present, see Figure 41 on page 93and follow these steps:

1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Show Active Alarms**.

At this point, the Active Alarms page displays all active alarms in the system, including VCG alarms, if present. The table contains a separate entry for each active VCG alarm. Table 43 describes the fields for each VCG alarm entry.

Table 43. Table Entries for Active VCG Alarms

Table Entry for Active Alarms	Field Value
Type	**VCG LOA, VCG LOM,** or **VCG SQM**
Alarm Raised Time	Date and time
Severity	Critical, Major, Minor, or Warning
Detailed Information	Location of affected VCG (VCG:*slot-number*)

Note The system automatically updates the Active Alarms page every 60 seconds. Click on Refresh if you need to update the table with the most recent active alarm information. Individual table entries automatically clear whenever previously active alarms are no longer present.

Table 44 provides a list of the GFP alarms that the system supports.

Table 44. GFP Alarms

Alarm	Description	Occurs when. . .
LFD	Loss of Frame Delineation	Multiple bit errors are detected in the Core Header by the cHEC
UPM	User Payload Mismatch	A mismatch occurs between the provisioned and received User Payload Identifiers (UPIs) in the GFP payload type field
EXM	Extension Header Mismatch	A mismatch occurs between the provisioned and received Extension Header Identifiers (EXIs) in the GFP payload type field

Displaying the Alarm Log

To display historical alarms, including any VCG or GFP alarms if present, follow these steps:

1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Show Alarm Log**.

At this point, the **Alarm Log** page displays a list of the 50 most recent alarm messages. The system keeps up to 500 entries in the alarm log.

> **Note** The alarm log is a FIFO (first-in fist-out) log.

Click on **Last 50 Log Entries** or **Next 50 Log Entries** to move around and display the entire contents of the log. Click on **Clear Log** if you wish to delete permanently the current log entries.

VCAT Group Performance Monitoring

Table 45 provides a list of the near-end PM parameters that the system monitors for VCAT groups (VCGs).

Table 45. VCG PM Parameters

Parameter	Description	Definition
VCG BBE	Background Block Error	Count of BBE across all VCG members
VCG ES	Errored Second	Count of seconds in which an ES occurs on one or more VCG members or in which the LOA, LOM, or SQM defect occurs
VCG SES	Severely Errored Second	Count of seconds in which an SES occurs on one or more VCG members or in which the LOA, LOM, or SQM defect occurs
VCG UAS	Unavailable Seconds	Period of unavailable time that begins at the onset of 10 consecutive SESs
LOAS	Loss of Alignment Seconds	Count of seconds in which the LOA defect occurs
LOMS	Loss of Multiframe Seconds	Count of seconds in which the LOM defect occurs
SQMS	Sequence Mismatch Seconds	Count of seconds in which the SQM defect occurs

To display current PM data for a VCG, see Figure 57 on page 123 and follow these steps:

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select **VCAT Groups**.
3. On the **VCAT Groups** page, select the VCG for which you wish to display the PM counts and click on **Show PM**.

At this point, the **VCAT Group Near-end PM** page (see Figure 57) shows the near-end PM data for both the current 15-minute and 24-hour periods.

> **Note** The PM data is not updated automatically as new events occur during the current 15-minute and 24-hour periods. Click on **Refresh** to update the tables with the most recent cumulative count for the current periods.

Continue with the steps that follow to display historical PM data.

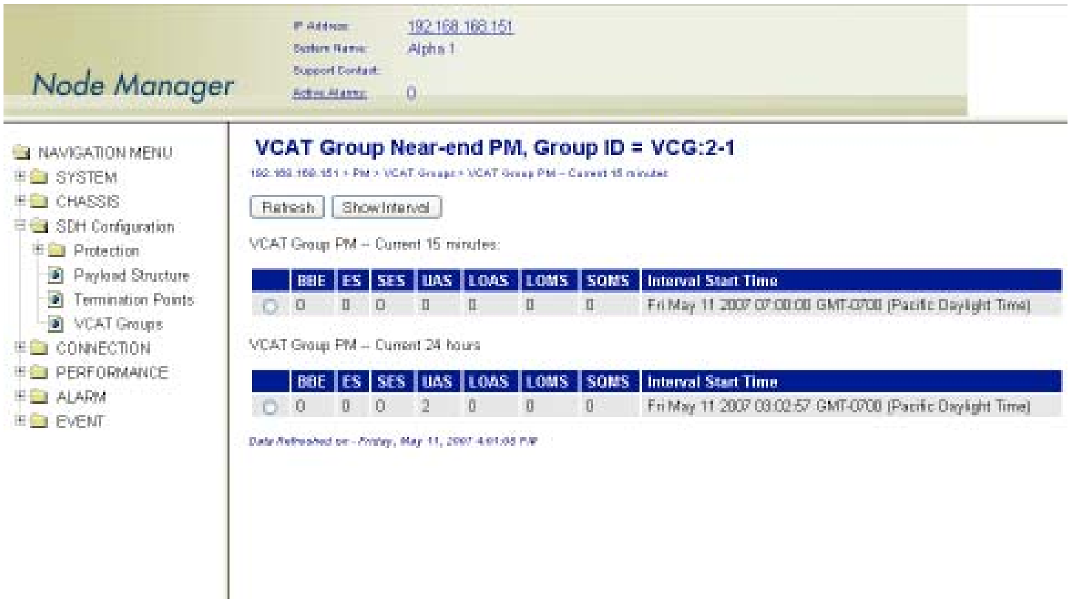
4. Click on **Show Interval**.

At this point, the **VCAT Group Near-end PM** page shows the near-end PM data for the following intervals:

- Current plus previous 95-by-15-minute intervals (24 hours total)
- Current plus previous day (2 days total)

Click on **Refresh** to update the tables with the most recent cumulative count for the current periods. This action updates only the first entry in the tables, which corresponds to the current measurement period.

Note The tables display **Invalid** under **PM data** when the data collected during a measurement period is considered invalid. The **Interval Start Time** also displays n/a (not available).



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

VCAT Group Near-end PM, Group ID = VCG:2-1

192.168.168.151 > PM > VCAT Groups > VCAT Group PM – Current 15 minutes

VCAT Group PM – Current 15 minutes:

	BBE	ES	SES	UAS	LOAS	LOMS	SQMS	Interval Start Time
○	0	0	0	0	0	0	0	Fri May 11 2007 07:00:00 GMT-0700 (Pacific Daylight Time)

VCAT Group PM – Current 24 hours

	BBE	ES	SES	UAS	LOAS	LOMS	SQMS	Interval Start Time
○	0	0	0	2	0	0	0	Fri May 11 2007 08:02:57 GMT-0700 (Pacific Daylight Time)

Data Refreshed on - Friday, May 11, 2007 4:01:05 PM

Figure 57. Displaying Current PM Data for VCGs

To display current and historical PM data for all VCGs in the system, see Figure 58 on page 124 and follow these steps:

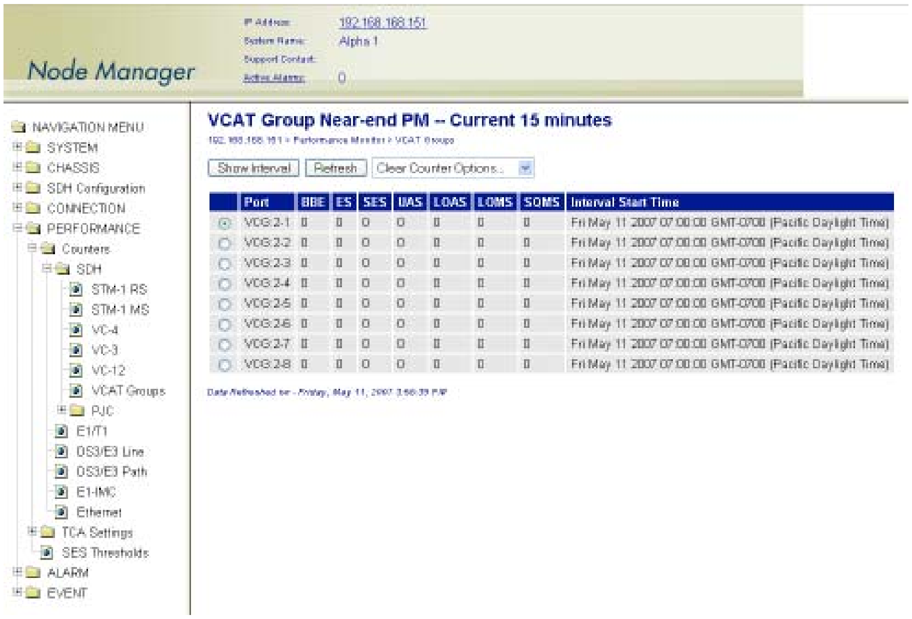
1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select **Counters**.
3. From the expanded **Counters** folder, select **SDH**.
4. From the expanded **SDH** folder, select **VCAT Groups**.

At this point, the **VCAT Group Near-end PM** – Current 15 minutes page shows the near-end PM data for the current 15-minute period only.

Continue with the steps that follow to display historical PM data for both 15-minute and 24-hour periods.

5. Select a VCG and click on **Show Interval**.

Note The preceding notes for the **VCAT Group Near-end PM** page also apply to this procedure.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

VCAT Group Near-end PM -- Current 15 minutes

192.168.168.151 > Performance Monitor > VCAT Groups

	Port	BBE	ES	SES	UAS	LOAS	LOMS	SQMS	Interval Start Time
●	VCG:2-1	0	0	0	0	0	0	0	Fri May 11 2007 07:00:00 GMT-0700 (Pacific Daylight Time)
○	VCG:2-2	0	0	0	0	0	0	0	Fri May 11 2007 07:00:00 GMT-0700 (Pacific Daylight Time)
○	VCG:2-3	0	0	0	0	0	0	0	Fri May 11 2007 07:00:00 GMT-0700 (Pacific Daylight Time)
○	VCG:2-4	0	0	0	0	0	0	0	Fri May 11 2007 07:00:00 GMT-0700 (Pacific Daylight Time)
○	VCG:2-5	0	0	0	0	0	0	0	Fri May 11 2007 07:00:00 GMT-0700 (Pacific Daylight Time)
○	VCG:2-6	0	0	0	0	0	0	0	Fri May 11 2007 07:00:00 GMT-0700 (Pacific Daylight Time)
○	VCG:2-7	0	0	0	0	0	0	0	Fri May 11 2007 07:00:00 GMT-0700 (Pacific Daylight Time)
○	VCG:2-8	0	0	0	0	0	0	0	Fri May 11 2007 07:00:00 GMT-0700 (Pacific Daylight Time)

Data Refreshed on - Friday, May 11, 2007 3:56:39 PM

Figure 58. Displaying Current PM Data for All VCGs

To clear the current PM data for a VCG, see Figure 58 and follow this step:

1. On the **VCAT Group Near-end PM** page, select one of the VCG entries and use the **Clear Counter Options...** scroll-down button to select one of the available options for clearing the current 15-minute counter, 24-hour counter, or both.

Link Capacity Adjustment Scheme (LCAS)

The system supports the use of the LCAS feature for VCGs in slots 2 and 3 only. (LCAS is not supported for VCGs is slot 1.) LCAS supports two basic functions:

- **Hitless addition and deletion of VCG members:** Dynamic adjustment of provisioned VCG bandwidth through manual commands issued from the OnSight Device Manager or the NMS.
- **Temporary removal of failed VCG members:** Automatic reduction of provisioned VCG bandwidth upon detection of failures in one or more VCG members. Maintains service connectivity over remaining non-failed VCG members. VCG bandwidth automatically restored as failed members return back to normal. Does not require intervention through the Device Manager or NMS.

To configure a VCG for LCAS operation, follow these steps:

1. In the Create VCAT Group window (see Figure 62), set LCAS to Enabled and click on Apply.

At this point, the VCG is enabled for LCAS operation.

Each VCG member has two LCAS components: a source (So) and a sink (Sk) component. When a VCG is first enabled for LCAS operation, the system automatically enables the LCAS (Sk) component for all current VCG members. At this point, the members begin processing and acting upon LCAS control words received at the sink side of the VCG. However, the system requires manual activation of the LCAS (So) component for individual VCG members. Upon activation of the source component, the selected members begin the generation of LCAS control words and become part of the composite VCG payload capacity at the source side of the VCG.

> **Note** Individual VCG members use the LCAS control packet to send and receive LCAS signaling information. The LCAS control packet contains the control (CTRL) word and the member status (MST) information for each VCG member. For VCGs at the VC-12 level, the LCAS control packet is located in the K4 byte bit 2 over multiple frames; and for VCGs at the VC-3 level, it is located in the H4 byte over multiple frames.

Table 46 provides a list of the LCAS control (CTRL) words that can be sent over LCAS control packets. MST has only two states: OK and FAIL.

Table 46. LCAS Control (CTRL) Words

Command	Indicates . . .
FIXED	This end uses fixed bandwidth (non-LCAS mode)
ADD	This member is about to be added to the group
NORM	Normal transmission
EOS	End of sequence and normal transmission
IDLE	This member is not part of the group or about to be removed
DNU	Do Not Use (the payload); the Sk side reported FAIL status

To create and add new members into the VCG, follow these steps:

1. On the **VCAT Groups** page, select the LCAS-enabled VCG that you wish to configure and click on **Properties**.
2. In the **VCAT Group Properties** window, click on **VCG Member Management**.

To provision additional TU timeslots for inclusion into the VCG, see Figure 59 on page 126 and continue with the rest of step 2 below. Otherwise, if the VCG already contains all the required member timeslots, continue with Step 3.

– In the VCG Member Management window, click on Create VCG Member.

– In the Create New Member in VCG window, select the Member Locations for each new VCG member.

The system highlights default member locations according to the number of VCG members that you select. You may, however, choose TU timeslots other than the default locations.

To select more than one member from the list, click on individual entries while pressing the Ctrl key. (The system highlights any entry that you select from the list. You can select any entry from the list, whether the member locations are contiguous or not.)

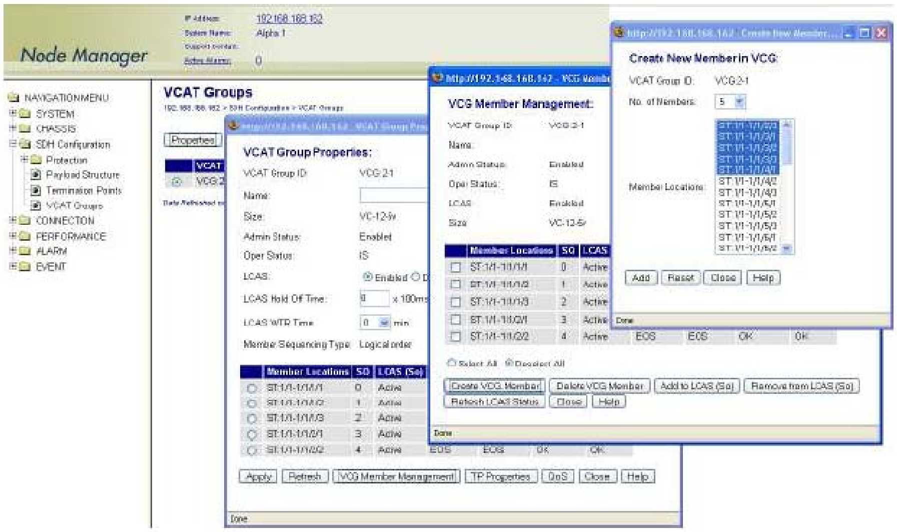
To select a range of consecutive entries from the list, select the first entry and then select the last entry while pressing the Shift key. Use the **Reset** button to restore the window to the default member location.

Note Make sure that the number of selected entries from the list matches the No. of Members before proceeding; otherwise, the system rejects the creation of new VCG members.

– Click on **Add** and then on **Close** to close the Create New Member in VCG window.

– Click on **Refresh LCAS Status** in the **VCG Member Management** window.

At this point, the newly-created members appear as part of the VCG in the **VCG Member Management** window. Also, the new VCG members begin processing and acting upon LCAS control words received at the sink side of the VCG.



VCAT Group Properties:

VCAT Group ID: VCG 2-1
Name:
Size: VC-12-5v
Admin Status: Enabled
Oper Status: IS
LCAS: ● Enabled ○ D
LCAS Hold Off Time: 0 x 100ms
LCAS WTR Time: 0 min
Member Sequencing Type: Logical order

	Member Locations	SQ	LCAS (So)
○	ST:1/1-1/1/1/1	0	Active
○	ST:1/1-1/1/1/2	1	Active
○	ST:1/1-1/1/1/3	2	Active
○	ST:1/1-1/1/2/1	3	Active
○	ST:1/1-1/1/2/2	4	Active

VCG Member Management:

VCAT Group ID: VCG 2-1
Name:
Admin Status: Enabled
Oper Status: IS
LCAS: Enabled
Size: VC-12-5v

	Member Locations	SQ	LCAS				
□	ST:1/1-1/1/1/1	0	Active				
□	ST:1/1-1/1/1/2	1	Active				
□	ST:1/1-1/1/1/3	2	Active				
□	ST:1/1-1/1/2/1	3	Active				
□	ST:1/1-1/1/2/2	4	Active	EOS	EOS	OK	OK

Create New Member in VCG:

VCAT Group ID: VCG 2-1
No. of Members: 5
Member Locations: ST:1/1-1/1/2/3, ST:1/1-1/1/3/1, ST:1/1-1/1/3/2, ST:1/1-1/1/3/3, ST:1/1-1/1/4/1 (selected), ST:1/1-1/1/4/2, ST:1/1-1/1/4/3, ST:1/1-1/1/5/1, ST:1/1-1/1/5/2, ST:1/1-1/1/5/3, ST:1/1-1/1/6/1, ST:1/1-1/1/6/2

Figure 59. Creating New VCG Members

3. In the **VCG Member Management** window, use the selector box to indicate the VCG members that you wish to include in the payload capacity at the source side of the VCG (see Figure 67).

At this point, **CTRL** (**So**) is **IDLE** for all inactive VCG members at the source side of the VCG. Also, the sequence (SQ) number for these members displays the maximum value of 63 for VCGs at the VC-12 level, and 255 for VCGs at the VC-3 level.

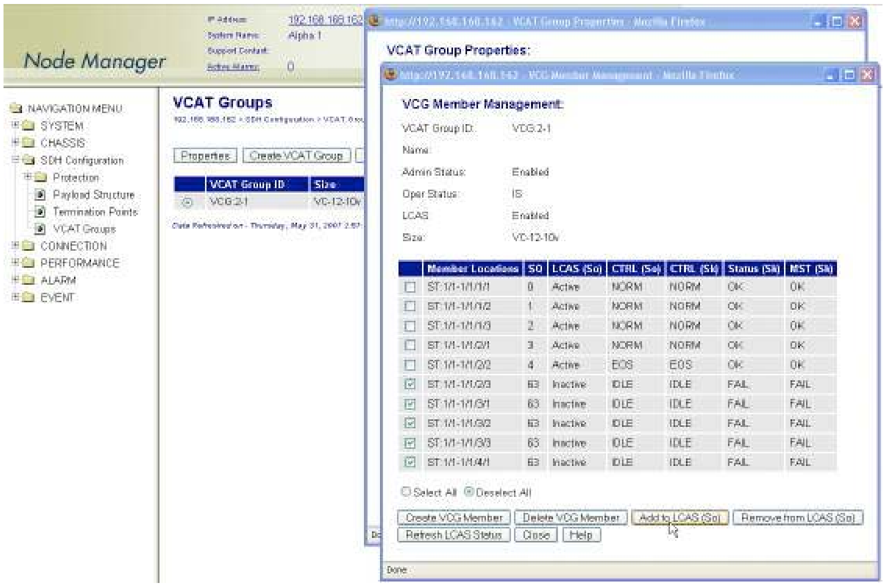
To select all VCG member entries in the table, click on **Select All** at the botton of the table. You can also click on **Deselect All** to clear all the selection boxes.

Note To ensure successful addition of new VCG members, it is necessary that there is SDH path connectivity between the timeslots that contain the new members on both sides of the endto- end VCG connection.

4. Click on the **Add to LCAS** (**So**) button (see Figure 60 on page 127).

At this point, **LCAS** (**So**) for the selected VCG members changes from **Inactive** to **Active,** and the selected members begin sending ADD in the transmit control word; that is, **CTRL** (**So**) = **ADD**. Also, the system automatically sets and displays the sequence (**SQ**) number for all active members at the source side of the VCG. For a VC-n-Xv, the SQ number for all members ranges from 0 to X-1.

Note The system sends the ADD control word in sequencial manner for each new active member on the source side of the VCG. That is, the first new active member sends ADD while the rest of the members remain IDLE. When the **MST** (**Sk**) for a new active member changes from FAIL to OK, **CTRL** (**So**) changes from ADD to NORM (or to EOS for the current last member). This change indicates the successful addition of the member into the composite VCG payload capacity at the source side of the VCG and the start of transmission of Ethernet packets over that member. In the same manner, the system continues with the automatic addition of new active members – one by one – until all new active members become part of the VCG at the source side.



VCG Member Management:

VCAT Group ID: VCG:2-1
Name:
Admin Status: Enabled
Oper Status: IS
LCAS Enabled
Size: VC-12-10v

	Member Locations	SQ	LCAS (So)	CTRL (So)	CTRL (Sk)	Status (Sk)	MST (Sk)
□	ST:1/1-1/1/1/1	0	Active	NORM	NORM	OK	OK
□	ST:1/1-1/1/1/2	1	Active	NORM	NORM	OK	OK
□	ST:1/1-1/1/1/3	2	Active	NORM	NORM	OK	OK
□	ST:1/1-1/1/2/1	3	Active	NORM	NORM	OK	OK
□	ST:1/1-1/1/2/2	4	Active	EOS	EOS	OK	OK
☑	ST:1/1-1/1/2/3	63	Inactive	IDLE	IDLE	FAIL	FAIL
☑	ST:1/1-1/1/3/1	63	Inactive	IDLE	IDLE	FAIL	FAIL
☑	ST:1/1-1/1/3/2	63	Inactive	IDLE	IDLE	FAIL	FAIL
☑	ST:1/1-1/1/3/3	63	Inactive	IDLE	IDLE	FAIL	FAIL
☑	ST:1/1-1/1/4/1	63	Inactive	IDLE	IDLE	FAIL	FAIL

○ Select All ● Deselect All

Figure 60. Adding VCG Members to the LCAS (So) Function

5. Check that **CTRL** (**So**) = **NORM** (or **EOS** if a member is the last in the sequence) and **MST** (**Sk**) = **OK** for all new active members at the source side of the VCG (see Figure 61 on page 128).

Note Click on **Refresh LCAS Status** to display the current value for each of the LCAS parameters. (You may need to continue refreshing the LCAS status until the system displays a status change for all selected members.)

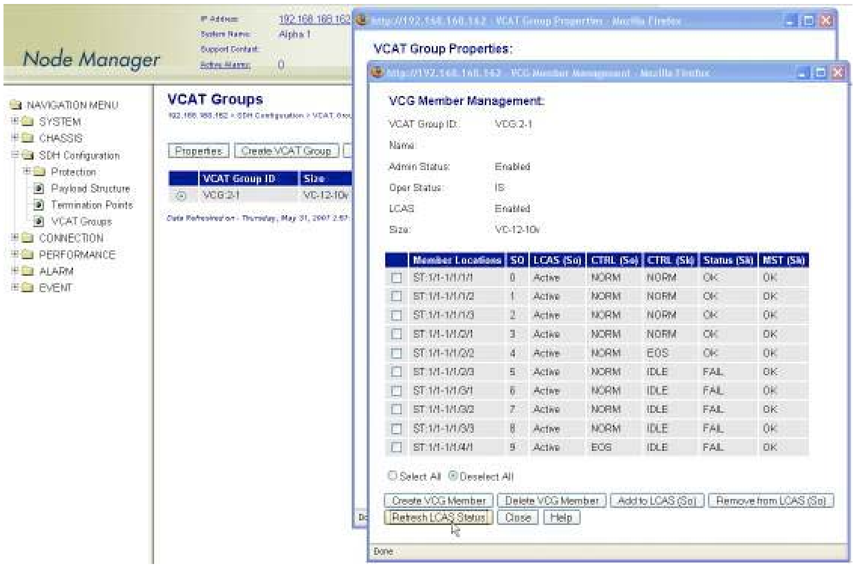
During the sequential addition process, the system skips any particular member that cannot be added unto the VCG at the source side because of a path connectivity or LCAS signaling failure. Failed active members – that is, members with **CTRL** (**So**) = **ADD** and **MST** (**Sk**) = **FAIL** – continue sending ADD until you select the members and press the **Remove from LCAS** button. This action changes the **CTRL** (**So**) word back to **IDLE** and stops the addition process for the selected member.

CAUTION

LCAS operations are unidirectional. This means that adding or removing VCG members in both directions of transmission requires repeating the “add” or “remove” procedure twice – once for each direction of transmission.

6. Click on **Close** to close the **VCG Member Management** window.

The **Size** field on the **VCAT Groups** page reflects the new size of the VCG after the creation of the VCG members.



VCG Member Management:

VCAT Group ID: VCG:2-1
Name:
Admin Status: Enabled
Oper Status: IS
LCAS: Enabled
Size: VC-12-10v

	Member Locations	SQ	LCAS (So)	CTRL (So)	CTRL (Sk)	Status (Sk)	MST (Sk)
☐	ST:1/1-1/1/1/1	0	Active	NORM	NORM	OK	OK
☐	ST:1/1-1/1/1/2	1	Active	NORM	NORM	OK	OK
☐	ST:1/1-1/1/1/3	2	Active	NORM	NORM	OK	OK
☐	ST:1/1-1/1/2/1	3	Active	NORM	NORM	OK	OK
☐	ST:1/1-1/1/2/2	4	Active	NORM	EOS	OK	OK
☐	ST:1/1-1/1/2/3	5	Active	NORM	IDLE	FAIL	OK
☐	ST:1/1-1/1/3/1	6	Active	NORM	IDLE	FAIL	OK
☐	ST:1/1-1/1/3/2	7	Active	NORM	IDLE	FAIL	OK
☐	ST:1/1-1/1/3/3	8	Active	NORM	IDLE	FAIL	OK
☐	ST:1/1-1/1/4/1	9	Active	EOS	IDLE	FAIL	OK

Figure 61. Completion of the Add to LCAS (So) Operation

To remove and delete members from the VCG, follow these steps:

1. On the **VCAT Groups** page, select the LCAS-enabled VCG that you wish to configure and click on **Properties**.

2. In the **VCAT Group Properties** window, click on **VCG Member Management**.

3. In the **VCG Member Management** window, use the selector box to indicate the VCG members that you wish to remove from the source side of the VCG.

To select all VCG member entries in the table, click on **Select All** at the botton of the table. You can also click on **Deselect All** to clear all the selection boxes.

At this point, **CTRL** (**So**) is **NORM** (or **EOS** for the last active member) for all active VCG members at the source side of the VCG. This control word indicates that the VCG members are configured for carrying Ethernet traffic in the So to Sk direction. Also, the SQ number for all active VCG members at the source side should range from 0 to X-1.

4. Click on the **Remove from LCAS** (**So**) button.

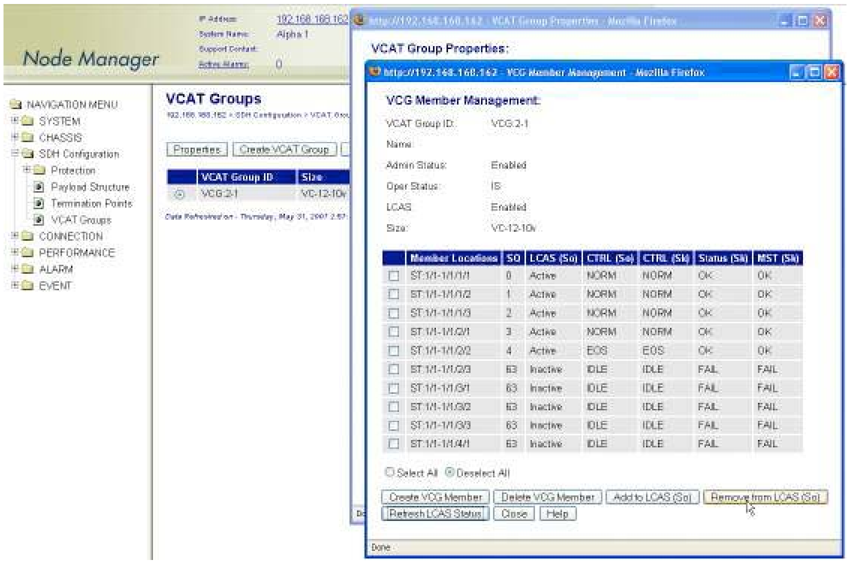
At this point, **LCAS** (**So**) for the selected VCG members changes from **Active** to **Inactive**, and the selected members begin sending IDLE in the source control word; that is, **CTRL** (**So**) = **IDLE**. Also, the system changes the SQ number for all inactive VCG members at the source to the maximum value of 64 for VCGs at the VC-12 level, and 255 for VCGs at the VC-3 level. This change indicates the successful removal of the members from the VCG at the source side and the stop of transmission of Ethernet packets over those members.

Note Upon reception of the IDLE control word, the LCAS processor at the far end of the connection stops receiving traffic over the idle VCG member and changes the MST status of that member to FAIL.

5. Check that **CTRL** (**So**) = **IDLE** and **MST** (**Sk**) = **FAIL** for all inactive members.

Note Click on **Refresh LCAS Status** to display the current value for each of the LCAS parameters. (You may need to continue refreshing the LCAS status until the system displays a status change for all selected members.)

CAUTION LCAS operations are unidirectional. This means that adding or removing VCG members in both directions of transmission requires repeating the "add" or "remove" procedure twice – once for each direction of transmission.



VCG Member Management:

VCAT Group ID: VCG:2-1

Name:

Admin Status: Enabled

Oper Status: IS

LCAS: Enabled

Size: VC-12-10v

	Member Locations	SQ	LCAS (So)	CTRL (So)	CTRL (Sk)	Status (Sk)	MST (Sk)
□	ST:1/1-1/1/1/1	0	Active	NORM	NORM	OK	OK
□	ST:1/1-1/1/1/2	1	Active	NORM	NORM	OK	OK
□	ST:1/1-1/1/1/3	2	Active	NORM	NORM	OK	OK
□	ST:1/1-1/1/2/1	3	Active	NORM	NORM	OK	OK
□	ST:1/1-1/1/2/2	4	Active	EOS	EOS	OK	OK
□	ST:1/1-1/1/2/3	63	Inactive	IDLE	IDLE	FAIL	FAIL
□	ST:1/1-1/1/3/1	63	Inactive	IDLE	IDLE	FAIL	FAIL
□	ST:1/1-1/1/3/2	63	Inactive	IDLE	IDLE	FAIL	FAIL
□	ST:1/1-1/1/3/3	63	Inactive	IDLE	IDLE	FAIL	FAIL
□	ST:1/1-1/1/4/1	63	Inactive	IDLE	IDLE	FAIL	FAIL

○ Select All ● Deselect All

Figure 62. Completion of the Remove from LCAS (So) Operation

If you wish to delete members from the VCG, continue with Step 5 below. Otherwise, go to Step 6 to finish this task.

– In the **VCG Member Management** window, use the selector box to indicate the VCG members that you wish to delete from the VCG.

To select all VCG member entries in the table, click on **Select All** at the botton of the table. You can also click on **Deselect All** to clear all the selection boxes.

– Click on **Delete VCG Member** to start the deletion process.

At this point, the deleted members disappear from the table.

Note To ensure successful completion of the deletion process, it is necessary that the system displays **IDLE** for both **CTRL (So)** and **CTRL (Sk)** of the selected VCG members. Otherwise, the system rejects the deletion request for the selected members.

6. Click on **Close** to close the **VCG Member Management** window.

7. Click on **Close** to close the **VCG Properties** window.

The **Size** field on the **VCAT Groups** page reflects the new size of the VCG after the removal of the VCG members.

VCQ QoS

When Ethernet flows from multiple sources are aggregated into a single VCG, it may be necessary to use the QoS functions of the VCG to ensure that individual packet flows are treated in accordance with userdefined priority markings for the application.

Each VCG on the high-density Ethernet (HD-ENET) expansion module has 4 transmission priority queues (0-3). Altogether, these queues can be configured in one of three packet scheduling modes: fair, strict priority (SP) and weighted fair queuing (WFQ).

Figure 63 shows an example of the use of QoS functions for the aggregation of Ethernet flows from multiple Ethernet ports into a single VCG. In this example, each ingress flow from a port is manually assigned to a different transmit queue. (See §11.3 for details on Ethernet flows and connections.) The QoS settings for the VCG specify the manner in which the packet scheduler of the VCG services the queues for transmission in the ingress direction of the VCG.

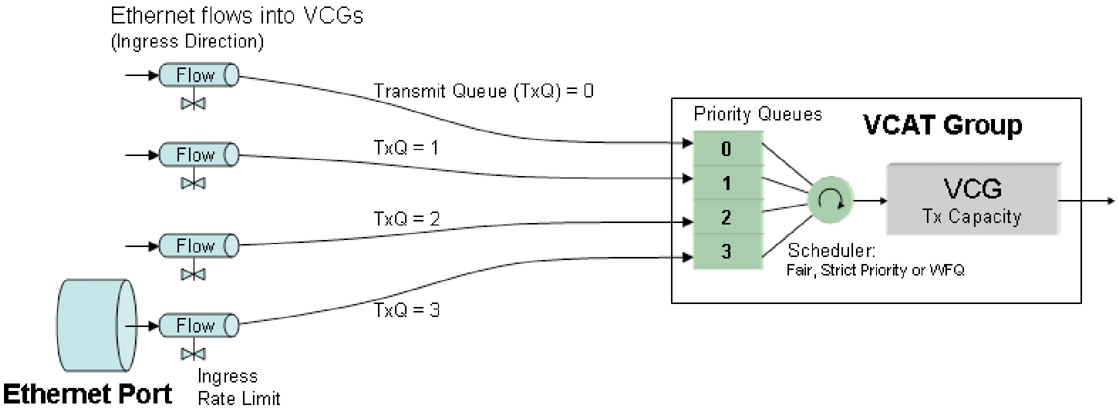


Figure 63. Application of VCG QoS for the Aggregation of Ethernet Flows into a VCG

To configure the QoS functions for a VCG, see Figure 64 and follow these steps:

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select **VCAT Groups**.
3. On the **VCAT Groups** page, select the VCG being configured and click on **Properties.**

> **Note** Only VCGs where the HD-ENET module is installed in slot 2 or 3 support configuration of the VCG QoS functions.

4. In the **VCAT Group Properties** window, click on **QoS**.
5. In the **VCG QoS Properties** window set **Queuing** to **Custom** if you wish to configure the packet scheduler of the VCG for operation in Strict Priority or WFQ mode.

To configure the packet scheduler in Strict Priority mode, continue with the first dash below; otherwise, for operation in WFQ mode, skip to the second dash.

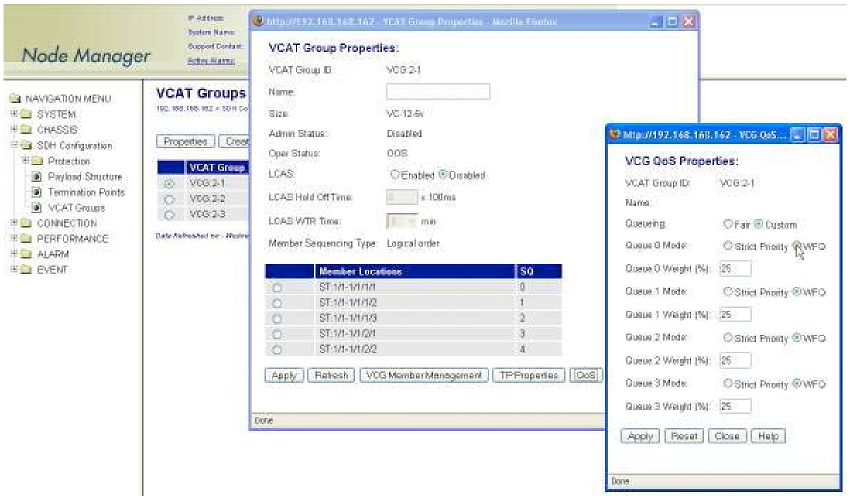
- To configure the packet scheduler of the VCG in **Strict Priority** mode, set **Queue 0 Mode** to **Strict Priority**. This change applies to all queues. (**Strict Priority** is the default setting for all queues.) Continue with Step 6 to complete this task.

In Strict Priority mode, the packet scheduler gives strict preference to packets in higher priority queues over packets in lower priority queues, regardless of the packet occupancy of individual queues. Among the four transmit queues, Queue 3 is the queue with the highest priority and Queue 0 is the queue with the lowest priority.

- To configure the packet scheduler of the VCG in **WFQ** mode, set **Queue 0 Mode** to **WFQ**. This change applies to all queues. Continue with Step 6 to complete this task.

In WFQ mode, the packet scheduler services the queues in accordance to a weight that you assign for each queue. The system requires that the sum of the weights for all four queues adds up to 100 percent.

6. Click on **Apply** and then on **Close** to close the **VCG QoS Properties** window.
7. Click on **Close** to close the **VCAT Group Properties** window.



VCAT Groups

	VCAT Group
●	VCG 2-1
○	VCG 2-2
○	VCG 2-3

VCAT Group Properties:

VCAT Group ID: VCG 2-1
Name:
Size: VC-12-5v
Admin Status: Disabled
Oper Status: OOS
LCAS: ○ Enabled ● Disabled
LCAS Hold Off Time: x 100ms
LCAS WTR Time: min
Member Sequencing Type: Logical order

	Member Locations	SQ
○	ST:1/1-1/1/1/1	0
○	ST:1/1-1/1/1/2	1
○	ST:1/1-1/1/1/3	2
○	ST:1/1-1/1/2/1	3
○	ST:1/1-1/1/2/2	4

http://192.168.168.162 - VCG QoS...

VCG QoS Properties:

VCAT Group ID: VCG 2-1
Name:
Queueing: ○ Fair ● Custom
Queue 0 Mode: ○ Strict Priority ● WFQ
Queue 0 Weight (%): 25
Queue 1 Mode: ○ Strict Priority ● WFQ
Queue 1 Weight (%): 25
Queue 2 Mode: ○ Strict Priority ● WFQ
Queue 2 Weight (%): 25
Queue 3 Mode: ○ Strict Priority ● WFQ
Queue 3 Weight (%): 25

Figure 64. Configuring the VCG QoS Functions

Subnetwork Connection Protection (SNCP)

The following section provides the procedures for provisioning and operating the OS-10 in subnetwork connection protection (SNCP) mode.

In SNCP mode, the two STM-1 ports in slot 1 (the base system) are designated as the “west” and “east” ports of the ADM node. STM-1 port 1 is the west port. STM-1 port 2 is the east port.

CAUTION

When setting up fiber connections in a ring, you must ensure that the west port of the ADM node connects to the east port of the adjacent ADM node. Continue the connection of ADM nodes in this manner until the ring topology is formed. This fiber connectivity is necessary to ensure proper operation of the ring (see Figure 65).

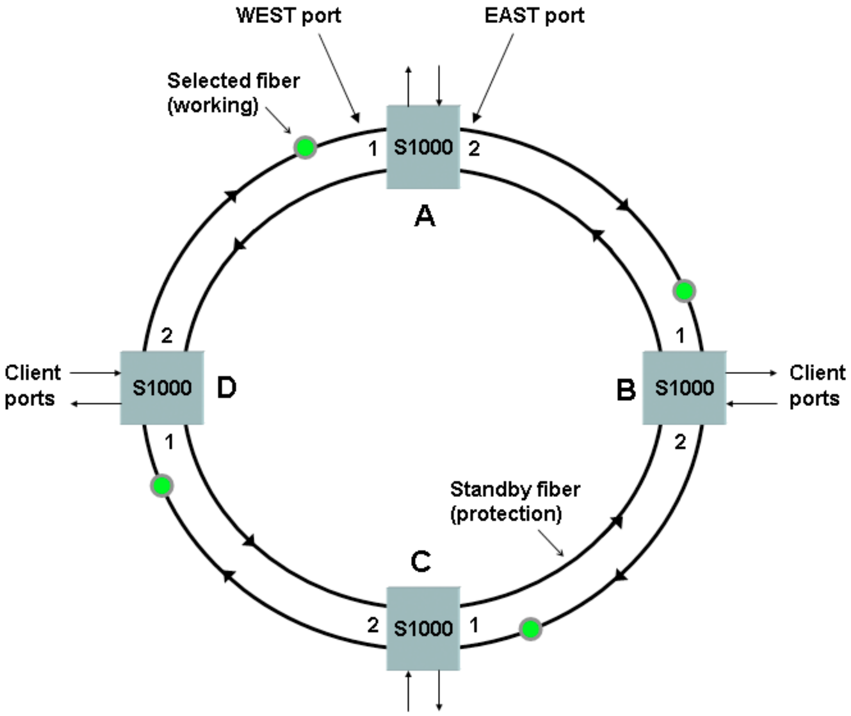


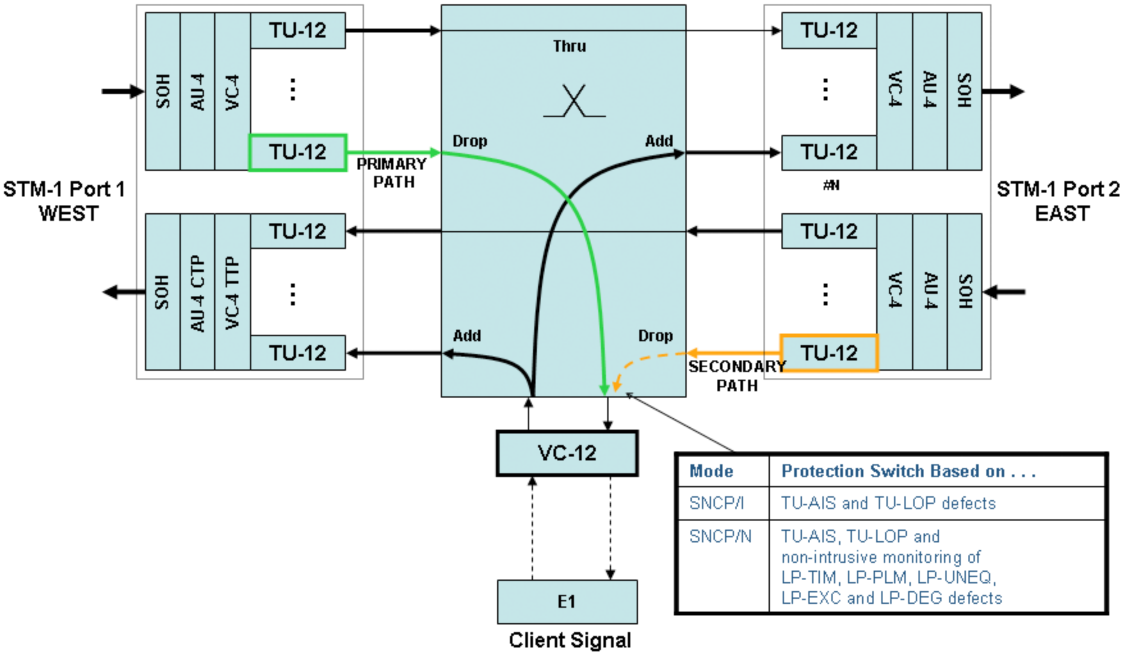
Figure 65. Ring ADM Interconnection Example

In a ring topology, the system uses SNCP to protect traffic against fiber cuts and node failures. The protection switch time is less than 50 msec.

The system supports operation in two SNCP modes: SNCP/I (inherent) and SNCP/N (non-intrusive). In the basic SNCP/I mode, VC-3 and VC-12 path selectors switch to a secondary path upon detection of TUAIS and TU-LOP defect on the primary path. In SNCP/N mode, VC-3 and VC-12 path selectors not only switch upon detection of TU-level defects (TU-AIS and TU-LOP) but also on low-order path (LP)-level defects: LP-PLM, LP-UNEQ, LP-TIM (if enabled), LP-EXC, and LP-DEG.

Figure 66 illustrates the internal system connections and switching criteria that support an E1 connection using SNCP/I or SNCP/N. In this example, when the SNCP mode is enabled, the system transmits a copy of the VC-12 that carries the E1 signal into both directions of transmission at the STM-1 level. That is, the system "adds" the VC-12 simultaneously over STM-1 port 1 (west port) and STM-1 port 2 (east port).

The transmitted VC-12 occupies the same TU-12 time slot location in both the east and west ports. In the "drop" direction, the system normally selects the received VC-12 copy from the same TU-12 time slot location in the "primary path." By default, the TU-12 that supports the "primary path" is located on the west port but you can set the TU-12 on the east port as the "primary path." If the "primary path" fails in accordance with the switching criteria for the selected SNCP mode (I or N), the system selects and drops the VC-12 copy from the "secondary path."



Mode	Protection Switch Based on . . .
SNCP/I	TU-AIS and TU-LOP defects
SNCP/N	TU-AIS, TU-LOP and non-intrusive monitoring of LP-TIM, LP-PLM, LP-UNEQ, LP-EXC and LP-DEG defects

Figure 66. SNCP Modes

By default, the system uses SNCP/N when a connection path is protected using SNCP. The system provides flexibility to configure individual paths for operation as SNCP/I or SNCP/N. You can use the SNCP feature for VC-3 or VC-12 path protection not only in a ring configuration but also in other network arrangements, such as a dual-homing configuration.

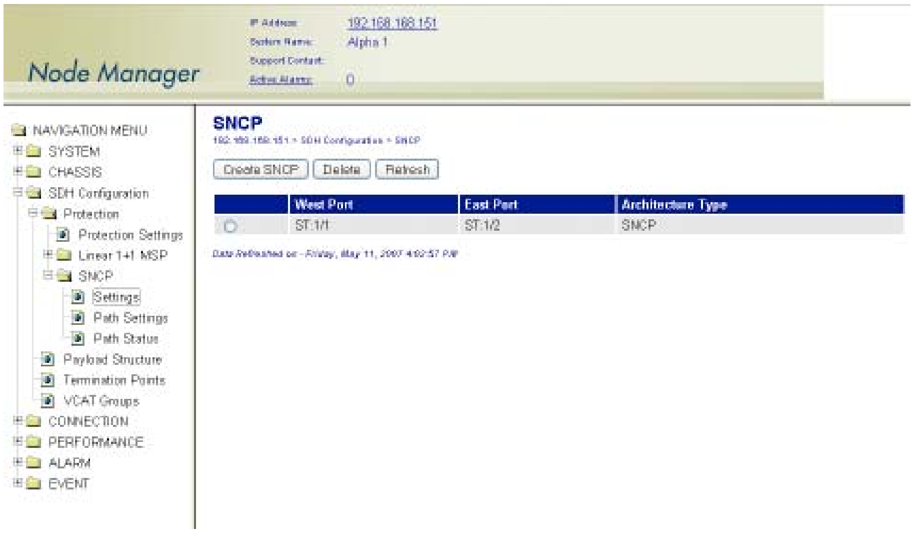
Provisioning STM-1 Ports in SNCP mode

To configure the STM-1 ports for operation in SNCP mode, see Figure 67 and follow these steps:

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select the **Protection** folder.
3. From the expanded **Protection** folder, select the **SNCP** folder.
4. From the expanded **SNCP** folder, select **Settings**.
5. On the **SNCP** page, select **Create SNCP**.
6. In the **SNCP Provisioning** window, select the STM-1 **West Port** and **East Port** pair from the available list of ports using the scroll-down button.
7. Click on **Apply** and then on **Close** to close the window.

On the **SNCP** page, the table now contains an entry with the selected STM-1 port pair configured for operation in SNCP mode.

Note The system rejects a request to configure the STM-1 ports in SNCP mode if the ports are already configured for operation in Linear 1+1 MSP mode or if the ports are configured as unprotected and connections, VCGs, or both are present.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

SNCP

192.168.168.151 > SDH Configuration > SNCP

	West Port	East Port	Architecture Type
○	ST:1/1	ST:1/2	SNCP

Data Refreshed on - Friday, May 11, 2007 4:02:57 PM

Figure 67. Configuring STM-1 Ports in SNCP Mode

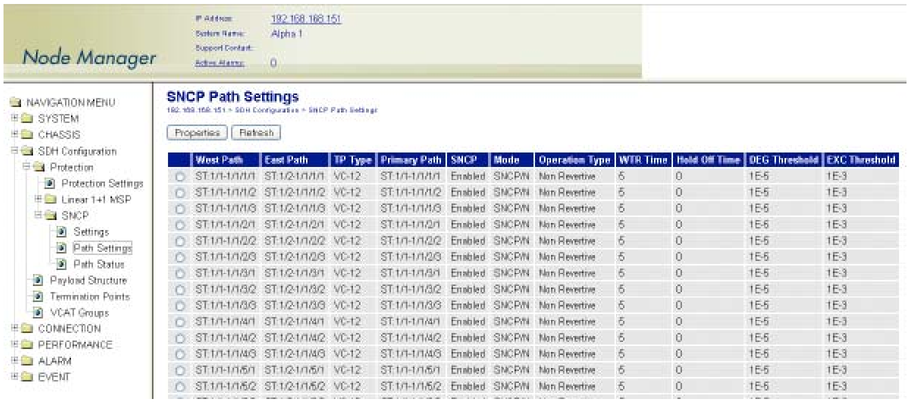
At this point, the system configures the SNCP path selectors in accordance with the payload structure of the STM-1 port pair. By default, the STM-1 ports are configured with 63 TU-12 time slots (21 TU-12 for each TUG-3).

Note The STM-1 payload structure must be the same for both the east and west ports (symmetry is required). The system ensures that both ports have the same payload configuration during the provisioning process.

Displaying and Configuring SNCP Path Settings

To display and configure the path settings for individual SNCP path selectors, see Figure 75 and follow these steps:

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select the **Protection** folder.
3. From the expanded **Protection** folder, select the **SNCP** folder.
4. From the expanded **SNCP** folder, select **Path Settings**.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

SNCP Path Settings

192.168.168.151 > SDH Configuration > SNCP Path Settings

	West Path	East Path	TP Type	Primary Path	SNCP	Mode	Operation Type	WTR Time	Hold Off Time	DEG Threshold	EXC Threshold
○	ST:1/1-1/1/1/1	ST:1/2-1/1/1/1	VC-12	ST:1/1-1/1/1/1	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/1/2	ST:1/2-1/1/1/2	VC-12	ST:1/1-1/1/1/2	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/1/3	ST:1/2-1/1/1/3	VC-12	ST:1/1-1/1/1/3	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/2/1	ST:1/2-1/1/2/1	VC-12	ST:1/1-1/1/2/1	Enabled	SNCP/N	Non Revertive	5	0	1E-6	1E-3
○	ST:1/1-1/1/2/2	ST:1/2-1/1/2/2	VC-12	ST:1/1-1/1/2/2	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/2/3	ST:1/2-1/1/2/3	VC-12	ST:1/1-1/1/2/3	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/3/1	ST:1/2-1/1/3/1	VC-12	ST:1/1-1/1/3/1	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/3/2	ST:1/2-1/1/3/2	VC-12	ST:1/1-1/1/3/2	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/3/3	ST:1/2-1/1/3/3	VC-12	ST:1/1-1/1/3/3	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/4/1	ST:1/2-1/1/4/1	VC-12	ST:1/1-1/1/4/1	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/4/2	ST:1/2-1/1/4/2	VC-12	ST:1/1-1/1/4/2	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/4/3	ST:1/2-1/1/4/3	VC-12	ST:1/1-1/1/4/3	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/5/1	ST:1/2-1/1/5/1	VC-12	ST:1/1-1/1/5/1	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3
○	ST:1/1-1/1/5/2	ST:1/2-1/1/5/2	VC-12	ST:1/1-1/1/5/2	Enabled	SNCP/N	Non Revertive	5	0	1E-5	1E-3

Figure 68. Displaying and Configuring the SNCP Path Settings

At this point, the **SNCP Path Settings** page displays the current SNCP path settings for each TU-3 and TU-12 time slot on the STM-1 ports. Table 47 provides a list of the parameters for each SNCP path.

> **Note** The system displays the table on the **SNCP Path Settings** page as empty when no ports are configured for operation in SNCP mode.

Table 47. SNCP Path Properties

Parameter	Definition
West Path	Location of VC-n path on the STM-1 west port.
East Path	Location of VC-n path on the STM-1 east port.
TP Type	Type of VC-n termination point: VC-3 or VC-12.
SNCP	SNCP protection indicator: enabled or disabled (disabled as default).
Mode	SNCP mode indicator: SNCP/I or SNCP/N.
Primary Path	Location of VC-n path from which the path selector normally drops traffic.
Operation Type	Path selector switch operation: revertive or non-revertive (nonrevertive as default).
WTR Time	Wait-to-restore time when path selector operates in revertive mode (1 to 12 minutes, with 5 minutes as default).
DEG Threshold	Wait-to-restore time when path selector operates in revertive mode (1 to 12 minutes, with 5 minutes as default).
EXC Threshold	Excessive error BER threshold when path selector operates in SNCP/N mode (1e-3 to 1e-5, with 1e-3 as default).

Table 47. SNCP Path Properties

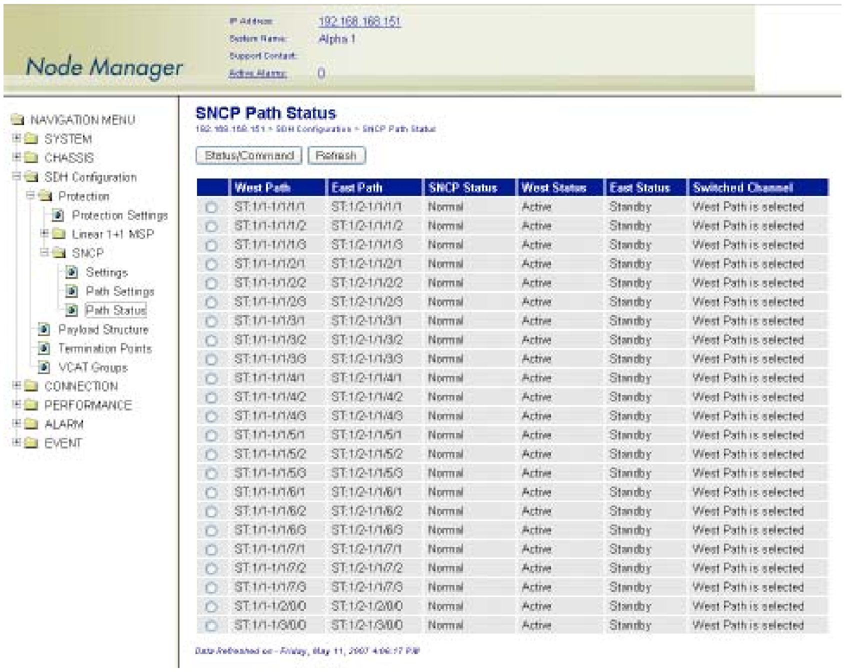
Parameter	Definition
Hold Off Time	Amount of time the path selector waits before switching from the primary to the secondary path in case of a failure in the primary path. The path selector switches to the secondary path only if the primary path is in the failed condition at the time the hold-off time expires. The timer is set in multiples of 100 msec, from 0 to 10 sec (0 sec as default).

By default, SNCP protection is disabled for each TU-3 and TU-12 time slot. You can enable SNCP protection for any time slot directly on the SNCP Path Settings page, or you may choose to enable SNCP protection as you create individual connections.

Displaying and Configuring SNCP Path Status

To display and configure the status of the SNCP path selector and the status of individual protected paths, see Figure 69 and follow these steps:

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select the **Protection** folder.
3. From the expanded **Protection** folder, select the **SNCP** folder.
4. From the expanded **SNCP** folder, select **Path Status**.



IP Address: 192.168.168.151
System Name: Alpha 1
Support Contact:
Active Alarms: 0

SNCP Path Status

192.168.168.151 > SDH Configuration > SNCP Path Status

	West Path	East Path	SNCP Status	West Status	East Status	Switched Channel
○	ST:1/1-1/1/1/1	ST:1/2-1/1/1/1	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/1/2	ST:1/2-1/1/1/2	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/1/3	ST:1/2-1/1/1/3	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/2/1	ST:1/2-1/1/2/1	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/2/2	ST:1/2-1/1/2/2	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/2/3	ST:1/2-1/1/2/3	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/3/1	ST:1/2-1/1/3/1	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/3/2	ST:1/2-1/1/3/2	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/3/3	ST:1/2-1/1/3/3	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/4/1	ST:1/2-1/1/4/1	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/4/2	ST:1/2-1/1/4/2	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/4/3	ST:1/2-1/1/4/3	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/5/1	ST:1/2-1/1/5/1	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/5/2	ST:1/2-1/1/5/2	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/5/3	ST:1/2-1/1/5/3	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/6/1	ST:1/2-1/1/6/1	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/6/2	ST:1/2-1/1/6/2	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/6/3	ST:1/2-1/1/6/3	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/7/1	ST:1/2-1/1/7/1	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/7/2	ST:1/2-1/1/7/2	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/1/7/3	ST:1/2-1/1/7/3	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/2/0/0	ST:1/2-1/2/0/0	Normal	Active	Standby	West Path is selected
○	ST:1/1-1/3/0/0	ST:1/2-1/3/0/0	Normal	Active	Standby	West Path is selected

Data Refreshed on - Friday, May 11, 2007 4:06:17 PM

Figure 69. Displaying and Configuring the SNCP Path Status

At this point, the **SNCP Path Status** page displays the current SNCP path status for each TU-3 and TU-12 time slot on the STM-1 ports. Table 48 on page 137 provides a list of the parameters for each SNCP path.

Note The system displays the table on the SNCP Path Settings page as empty when no ports are configured for operation in SNCP mode.

Table 48. SNCP Path Status

Parameter	Indicates. . .
West Path	Location of VC-n path on the west port
East Path	Location of VC-n path on the east port
SNCP Status	Status of SNCP selector: normal, lockout, forced, manual, signal failure and signal degrade
West Status	Status of VC-n path on the west port: active, standby, or failed
East Status	Status of VC-n path on the east port: active, standby, or failed
Switched Channel	Dropped channel selected by the path selector: east or west

Note The system displays N/A (Disabled) if SNCP protection is disabled for the time slot.

External Commands for SNCP Path Switching

The system allows the use of external commands to switch between east and west paths in SNCP configuration. Table 49 provides a list of the external commands that the system supports:

Table 49. External Commands for SNCP Path Switching

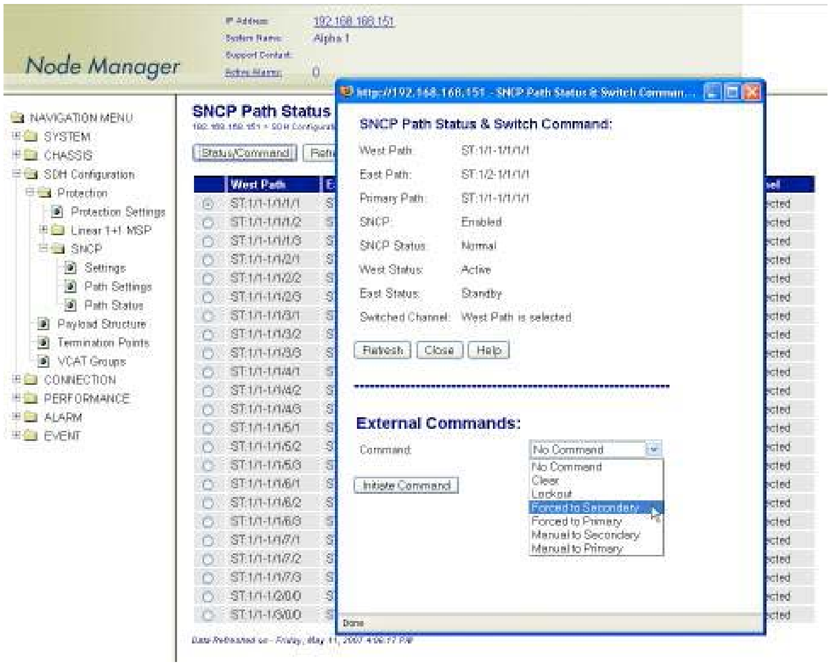
Priority	Command	Action	Completion
1	Clear	Clears all switch commands	Always
2	Lockout	Disables a switch to the protection path	Always
3	Forced to Secondary	Switches from the primary to the secondary path	Denied if the SF condition is present on the secondary path or if the Lockout command is present
	Forced to Primary	Switches from the secondary to the primary path	Denied if the Lockout command is present
4	Manual to Secondary	Switches from the primary to the secondary path	Denied if the SF or SD condition is present on the secondary path or if the Lockout or Forced command is present
	Manual to Primary	Switches from the secondary to the primary path	Denied if the SF or SD condition is present on the primary path or if the Lockout or Forced command is present

To activate any of the external commands for SNCP path switching, see Figure 70 and follow these steps:

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select the Protection folder.
3. From the expanded **Protection** folder, select the **SNCP** folder.
4. From the expanded **SNCP** folder, select **Path Status**.
5. On the **SNCP Path Status** page, select the table entry for the path for which you wish to activate the expernal commands and click on **Status/Command**.

> **Note** The system supports the activation of the external commands only for paths in which SNCP protection is enabled.

6. In the **SNCP Path Status & Switch Command** window, use the scroll-down button to select one of the **Command** options in Table 49 on page 137. By default, Command is set to No Command.
7. Click on **Initiate Command** to activate the external command.
8. To reset any active command, select the **Clear** command option and click on **Initiate Command**. Otherwise, the current command remains active until a higher-priority command is issued or failure occurs (see Figure 70).



IP Address: 192.168.168.151
System Name: Alpha 1
Active Alarms: 0

West Path
ST:1/1-1/1/1/1
ST:1/1-1/1/1/2
ST:1/1-1/1/1/3
ST:1/1-1/1/2/1
ST:1/1-1/1/2/2
ST:1/1-1/1/2/3
ST:1/1-1/1/3/1
ST:1/1-1/1/3/2
ST:1/1-1/1/3/3
ST:1/1-1/1/4/1
ST:1/1-1/1/4/2
ST:1/1-1/1/4/3
ST:1/1-1/1/5/1
ST:1/1-1/1/5/2
ST:1/1-1/1/5/3
ST:1/1-1/1/6/1
ST:1/1-1/1/6/2
ST:1/1-1/1/6/3
ST:1/1-1/1/7/1
ST:1/1-1/1/7/2
ST:1/1-1/1/7/3
ST:1/1-1/2/0/0
ST:1/1-1/3/0/0

Data Refreshed on - Friday, May 11, 2007 4:06:17 PM

http://192.168.168.151 - SNCP Path Status & Switch Comman...

SNCP Path Status & Switch Command:

West Path: ST:1/1-1/1/1/1
East Path: ST:1/2-1/1/1/1
Primary Path: ST:1/1-1/1/1/1
SNCP: Enabled
SNCP Status: Normal
West Status: Active
East Status: Standby
Switched Channel: West Path is selected

External Commands:

Command: No Command

Figure 70. Configuring the External Commands for SNCP Path Switching

Creating Cross-Connections

A cross-connection is a connection that supports time slot interchange (TSI) between any two STM-1 ports. This type of connection does not involve the mapping or demapping of client signal ports. As shown in Table 50, the OS-10 system supports two types of cross-connection: VC-3 and VC-12. Each cross-connection is characterized by three parameters: source, sink and direction. The STM-1 ports that contain the source and sink locations may be located in different slots in the system and need not use the same protection mode. For example, you may set up a VC-12 cross-connection between STM-1 base ports 1 and 2 in slot 1 operating in SNCP mode and STM-1 expansion ports 1 and 2 in slot 2 operating in Linear 1+1 MSP mode. You may also set up cross-connections between STM-1 ports in the same slot.

Table 50. Cross-Connection Types

Level	Source	Sink	Direction
VC-3	TU-3 in STM-1 port 1	TU-3 in STM-1 port 2	2-way
VC-12	TU-12 in STM-1 port 1	TU-12 in STM-1 port 2	2-way

For cross-connections, the system does not require that you use the same time slot locations (U/K/L/M) for the source and sink points. All cross-connections are 2-way (or bidirectional) crossconnections by default. This means that the relationship between the source and sink points is the same for both directions of transmission. After the direction from source to sink is specified, the reverse direction is implicitly defined by the 2-way nature of the connection.

To create cross-connections at the VC-12 level, see Figure 71 on page 140 and follow these steps:

1. Select the **CONNECTION** folder from the navigation menu.
2. From the expanded **CONNECTION** folder, select **Cross-Connections**.
3. On the **Cross-Connections** page, click on **Create Cross-Connection**.
4. In the **Create Cross-Connection** window, set **Level** to **VC-12**.
5. Select the source STM-1 port using the **STM-1 port** (**Source**) scroll-down button.

The system displays only the first STM-1 port of a protected pair in a slot operating in SNCP or Linear 1+1 MSP mode. The scroll-down list includes both ports in a slot (STM-1 ports 1 and 2) if the ports operate in unprotected mode. The list also includes more than one STM-1 port if the system contains STM-1 expansion ports in slots 2 and 3.

The **Protection Type** indicates the protection mode for the selected port.

6. Select the TU-12 location or locations for the source using the **TU-12 Location** (**Source**) scrolldown button.
7. Select the sink STM-1 port using the **STM-1 port** (**Sink**) scroll-down button.
8. Select the TU-12 location or locations for the sink using the **TU-12 Location** (**Sink**) scroll-down button.

To select more than one TU-12 location from the **TU-12 Location...** list, click on individual entries while pressing the Ctrl key. (The system highlights any entry that you select from the list. You can select any entry from the list, whether the TU-12 locations are contiguous or not.)

To select a range of consecutive entries from the list, select the first entry and then select the last entry while pressing the Shift key. Use the Reset button to restore the window to the default selection.

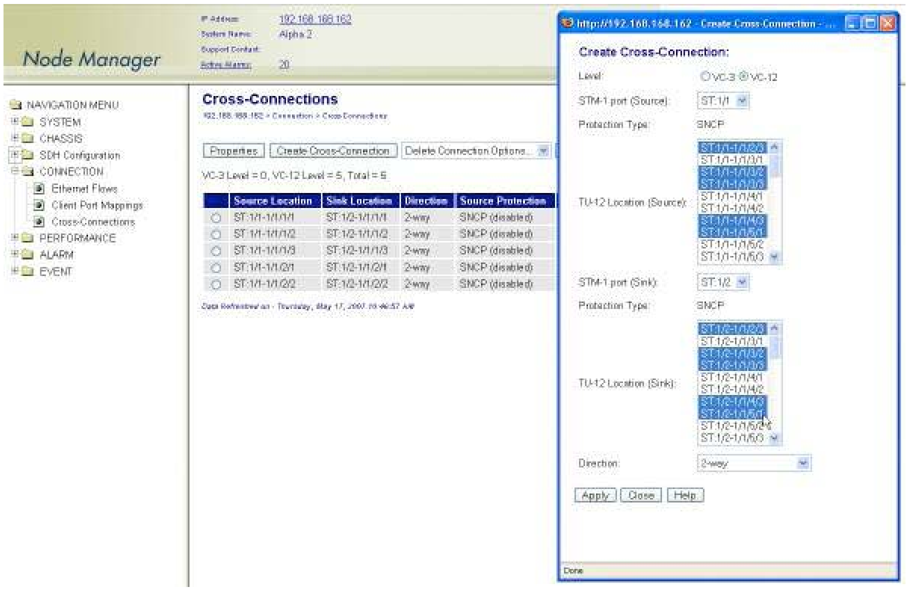
Note Make sure that the number of selected entries from the **TU-12 Location (Sink)** list matches the number of selected TU-12s in the **TU-12 Location (Source)** before proceeding; otherwise, the system rejects the creation of the cross-connections.

9. Click on **Apply** to initiate the creation of the VC-12 cross-connections.

CAUTION

The **Create Cross-Connection** window closes automatically after the system completes the creation of the VC-12 cross-connections. If the number of cross-connections is large, the system may take a few seconds to create the cross-connections and close the window. Closing the window manually before.the process is complete may cause an error or partial creation of the new cross-connections. Click on Refresh on the Cross-Connections page to update the cross-connect table with the new connections after the window closes.

To create cross-connections at the VC-3 level, set **Level** to **VC-3** in Step 4, and select the TU-3 location or locations for the source and sink points in the Create Cross-Connection window. The preceding notes and tips for TU-12 locations also apply to TU-3 locations.



Cross-Connections

192.168.168.162 > Connection > Cross-Connections

VC-3 Level = 0, VC-12 Level = 5, Total = 5

	Source Location	Sink Location	Direction	Source Protection
○	ST:1/1-1/1/1/1	ST:1/2-1/1/1/1	2-way	SNCP (disabled)
○	ST:1/1-1/1/1/2	ST:1/2-1/1/1/2	2-way	SNCP (disabled)
○	ST:1/1-1/1/1/3	ST:1/2-1/1/1/3	2-way	SNCP (disabled)
○	ST:1/1-1/1/2/1	ST:1/2-1/1/2/1	2-way	SNCP (disabled)
○	ST:1/1-1/1/2/2	ST:1/2-1/1/2/2	2-way	SNCP (disabled)

Data Refreshed on - Thursday, May 17, 2007 10:46:57 AM

Create Cross-Connection:

Level: ○ VC-3 ● VC-12

STM-1 port (Source): ST:1/1

Protection Type: SNCP

TU-12 Location (Source): ST:1/1-1/1/2/3, ST:1/1-1/1/3/1, ST:1/1-1/1/3/2, ST:1/1-1/1/3/3, ST:1/1-1/1/4/1, ST:1/1-1/1/4/2, ST:1/1-1/1/4/3, ST:1/1-1/1/5/1, ST:1/1-1/1/5/2, ST:1/1-1/1/5/3

STM-1 port (Sink): ST:1/2

Protection Type: SNCP

TU-12 Location (Sink): ST:1/2-1/1/2/3, ST:1/2-1/1/3/1, ST:1/2-1/1/3/2, ST:1/2-1/1/3/3, ST:1/2-1/1/4/1, ST:1/2-1/1/4/2, ST:1/2-1/1/4/3, ST:1/2-1/1/5/1, ST:1/2-1/1/5/2, ST:1/2-1/1/5/3

Direction: 2-way

Figure 71. Creating VC-12 Cross-Connections

Ring Operations

This section provides options for the synchronization of OS-10 nodes in a ring topology and the procedures for adding and removing OS-10 nodes into and from a ring.

Ring Synchronization

The OS-10 provides the following options for ring synchronization:

- **Option 1:** The head-end node of the ring is an OS-10 that uses external timing inputs at 2.048 MHz from a PRC-traceable source. All other nodes in the ring are OS-10 nodes set for STM-1 line timing. All nodes are set to process and generate synchronization status messaging (SSM).
- **Option 2:** The head-end node of the ring is an OS-10 node set in free-run mode using the internal Stratum 3 clock. All other nodes in the ring are OS-10 nodes set for STM-1 line timing. All nodes are set to process and generate SSM.

Option 2 may be used in applications where PRC-traceable source is not available at any site in the ring.

- **Option 3:** The head-end node of the ring is a third-party SDH node that uses timing from a PRCtraceable source. All other nodes in the ring are OS-10 nodes set for STM-1 line timing. All nodes in the ring are set to process and generate the SSM.

Adding and Deleting OS-10 Nodes

The following section provides the procedures for the addition and deletion of OS-10 nodes into and from a ring.

Adding OS-10 Nodes into a Ring

To add a new OS-10 node into a ring, follow these steps:

1. Install and power up the node that is being added into the ring.
2. Configure the system information, the Ethernet LAN management port, and system clock.
3. Configure the system for SNCP operation.
4. Configure the inband management channels for operation using the DCC.

Note Make sure that the DCC settings are compatible with the settings for the other nodes in the ring.

5. Set the system timing mode to Auto using the STM-1 ports as primary and secondary timing references.

Note This configuration is the same as STM-1 line timing.

CAUTION

Do not enable the STM-1 ports at this time. Wait until Step 11. Enabling the ports at this time may cause loss of traffic for existing connections when the new node is connected to the adjacent nodes using the fiber optic cables (see Step 8 and Step 10).

6. Set up cross-connections for all TU-3 and TU-12 time slots that are being used in the ring.

CAUTION

The TU-3 and TU-12 cross-connections are required to support existing connections in the ring. If the cross-connections are not present at the moment the node goes into service in the ring, traffic loss occurs for existing connections.

7. Disconnect the fiber optic cables that connect the two nodes adjacent to the new node.

Note Fiber disconnection should occur at the site where the new node is being put into service. Make sure that the ends of the fiber have SC connectors before proceeding with Step 8. You may need to install the SC connectors if a fiber patch panel that uses this connector type is not present at the site.

At this point, the two adjacent nodes perform a protection switch to protect existing traffic in the ring.

WARNING

At this point, any additional failure in ring may result in the loss of traffic for existing connections.

8. Connect the ring fiber optic cables only to the receive side of the east and west STM-1 ports of the new node. Leave the transmit side of the ports disconnected.

Note Follow the procedure in "Subnetwork Connection Protection (SNCP)" on page 132 to connect the STM-1 ports of the new node to the STM-1 ports of the adjacent nodes. That is, port 1 (west) of one node should connect to port 2 (east) of another node.

Use the J0 trace to ensure that fiber connectivity is correct between adjacent nodes.

CAUTION

Make sure that the optical signal power level from the fiber that connects to the receive side of the port is within the limits in Table 33 for the interface type that is being used (S-1.1 or L-1.1) You may need to use an optical attenuator to prevent receiver overload if the fiber span is short.

9. Check that the system timing status is "normal" and that sync quality level for either the primary or secondary reference is other than DNU, or "do not use".

At this point, the system should synchronize to one of the two incoming STM-1 signals. If the sync quality level for both references is DNU, the node is not properly synchronized to the other ring nodes.

Note Do not proceed until the sync quality level for at least one of the references is other than DNU.

10. Connect the ring fiber optic cables to the transmit side of the east and west STM-1 ports of the new node.

11. Enable STM-1 port 1 (west) and port 2 (east) at the same time.

12. Confirm that the new node is reachable through the DCC channels and that existing traffic is not affected.

At this point, you may now set up connections between the client ports of the new node and other nodes in the ring.

Removing OS-10 Nodes from a Ring

To remove an OS-10 node from a ring, follow these steps:

1. Remove all connections associated to the node that needs to be removed (or taken out of service).

> **Note** This procedure includes connections between the node that is being removed and other nodes in the ring.

2. Power down the node and disconnect the node from its power source (AC or DC).

> CAUTION
>
> Follow the safety precautions found in "Safety when using electricity" on page 14 and the *OnSite Series User Manual* when working with AC or DC power connected to the system.

> **Note** At this point, the two nodes adjacent to the node that is being removed perform a protection switch to protect the rest of the traffic in the ring.

> WARNING
>
> **At this point, any additional failure in ring may result in the loss of traffic for existing connections.**

3. Remove the fiber cables from STM-1 port 1 (west) and port 2 (east).

4. Patch through the fiber cables to restore fiber connectivity between the nodes adjacent to the node that is being removed.

> CAUTION
>
> Follow the safety precautions in "Optical Safety" on page 15 when working with fiber optic cables and laser devices.

> **Note** The procedure does not disrupt remaining traffic in the ring for more than 50 msec.

Linear ADM (2-Fiber)

To configure the OS-10 system for operation in 2-fiber (unprotected) Linear ADM mode, the two STM-1 ports on the base system must be configured as unprotected. In general, each unprotected STM-1 port may work independently from the other and can be configured with different payload structures (see "Configuring the SDH Payload Structure" on page 83). However, for proper operation of OS-10 nodes in a 2-fiber Linear ADM topology, it is important that you use the same payload structure for the east and west directions of transmission.

CAUTION

When setting up fiber connections in a linear ADM chain, you must ensure that the west port of the ADM node (STM-1 port 1) connects to the east port (STM-1 port 2) of the adjacent ADM node. Continue the connection of ADM nodes in this manner until the linear topology is formed. This fiber connectivity is necessary to ensure proper operation of the linear network.

You can map and connect traffic from any E1/T1 client port to any available TU-12 time slot in either STM-1 port.

Note When the STM-1 ports operate in unprotected mode, the **TU-12 Location** list includes the available TU-12 time slots for both STM-1 port 1 and port 2. In contrast, the **TU-12 Location** list for the Linear 1+1 MSP mode includes only the available TU-12 locations for port 1 (because of the requirement for time slot symmetry in this mode).

You can also map and connect traffic from any Ethernet client port to any available VCAT group (VCG) in either STM-1 port. To create VCGs at VC-3 and VC-12 levels, see "Creating a VCG" on page 110.

Note When the STM-1 ports operate in unprotected mode, the **Member Locations** list includes the available TU-3 and TU-12 time slots for both STM-1 port 1 and port 2.

In general, VC-3 and VC-12 cross-connections do not require time slot symmetry between unprotected STM-1 ports. That is, the U/K/L/M index for the source and sink need not be the same. However, for proper operation of OS-10 nodes in a 2-fiber Linear ADM topology, it is important that you use timeslot symmetry for all cross-connections.

Interconnection of OS-10 Nodes in a 2-Fiber Linear ADM Topology

As shown in Figure 72 on page 145, a linear ADM chain of three OS-10 nodes must start from STM-1 port 1/2 (ST:1/2) at the Headend node. This port should be connected to STM-1 port 1/1 (ST:1/1) of the first Intermediate node and ST:1/2 of this node should be connected to ST:1/1 of the next node in the chain (the End node).

Note Both port ST:1/1 of the Headend node and port ST:1/2 of the End node are not used in this network and must be disabled.

In general, there can be more than one Intermediate node in a linear ADM. Therefore, all linear ADM chains must start with ST:1/2 at the Headend node and end with ST:1/1 at the End node, and all Intermediate notes must connect to each other using an alternating sequence of STM-1 ports 1 and 2.

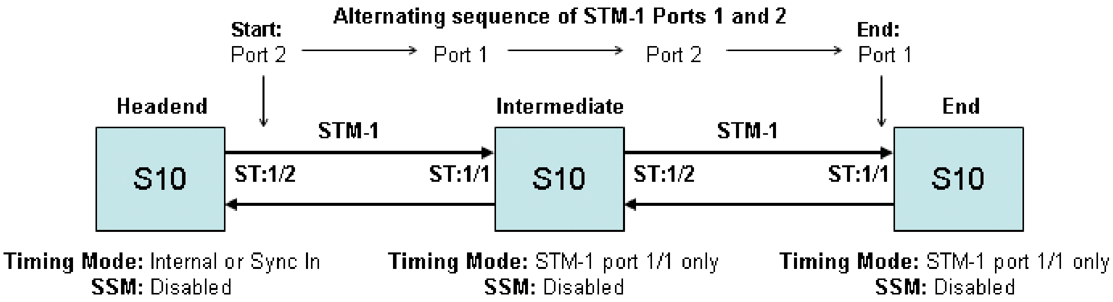

Start:
Port 2
Alternating sequence of STM-1 Ports 1 and 2
Port 1
Port 2
End:
Port 1
Headend
Intermediate
End
STM-1
STM-1
S10
S10
S10
ST:1/2
ST:1/1
ST:1/2
ST:1/1
Timing Mode: Internal or Sync In
SSM: Disabled
Timing Mode: STM-1 port 1/1 only
SSM: Disabled
Timing Mode: STM-1 port 1/1 only
SSM: Disabled

Figure 72. OS-10 Operation in 2-Fiber (Unprotected) Linear ADM Mode

Synchronization of OS-10 Nodes in a 2-Fiber Linear ADM Topology

All OS-10 nodes in a 2-fiber (unprotected) linear ADM chain must be synchronized to the Headend node. To perform this network synchronization arrangement, the following timing configuration rules apply (as shown in Figure 72):

- The Headend node must use either its own Internal clock (Stratum 3) or an external timing source connected to the Sync In port
- The Intermediate and End nodes must use STM-1 port 1 as the only timing source for the system. With this setting, the system goes immediatetly into holdover mode when STM-1 port 1 becomes unavailable as a timing referece
- All nodes must have the synchronization status messages (SSM) function disabled (see Figure 19 on page 55)

This configuration must be used for proper operation of OS-10 nodes in a 2-fiber (unprotected) linear ADM topology.

Chapter 4 **E1/T1 Interface**

Chapter contents

Introduction

This chapter provides the procedures for provisioning, monitoring and testing of E1 and T1 client signal ports. Procedures for connecting E1 and T1 traffic to SDH are also provided.

General Information

The OnSite OS-10 has 8 built-in E1 ports on the base OS1052 and 21 built-in E1 ports on the base OS1063 systems. E1 traffic is mapped into a VC-12 using asynchronous mapping, as specified in ITU-T Recommendation G.707. The VC-12 is multiplexed into an STM-1 through the AU-4 multiplexing route, as shown in Figure 73.

As a factory-installed option, the OS-10 is also available with 8 built-in T1 ports on the base OS1052 and 21 built-in T1 ports on the base OS1063 systems. T1 traffic is mapped into VC-11 containers using asynchronous mapping, as specified in G.707. The system connects VC-11s carrying T1 traffic into TU-12 time slots, as shown in Figure 73.

Note Asynchronous mapping supports clear-channel transport of G.703 services at 2.048 Mbit/s ± 50 ppm for E1 signals and at 1.544 Mbit/s ± 32 ppm for T1 signals.

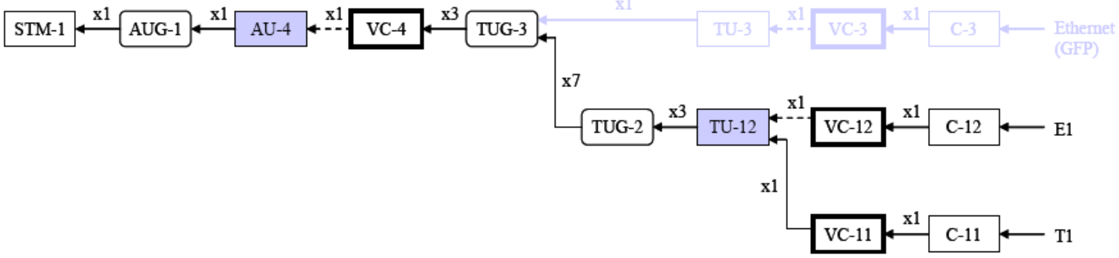


Figure 73. E1 and T1 Multiplexing over SDH

The E1 and T1 interfaces comply with the following standards:

- ITU-T G.703 (physical layer)
- ITU-T G.707 (SDH mapping)
- ITU-T G.775 (LOS detection)
- ITU-T G.826 (performance monitoring)
- ITU-T G.823 and G.783 (jitter and wander)

Figure 74 shows the location of the E1 and T1 ports on the base OS1052 and OS1063 systems.

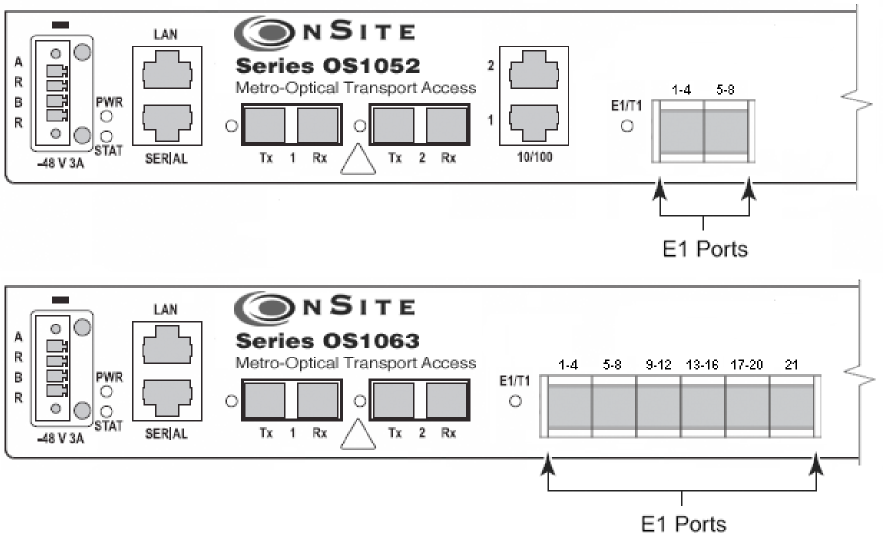


Figure 74. E1 and T1 Ports on the Base OS1052 and OS1063 Systems

The OS1052 and OS1063 also allow the insertion of a 21-port E1 expansion module for applications that require access to additional E1 ports (see chapter 12 for details on the HD-E1 module); with two expansion modules, the OS1052 suports a total of 52 E1 ports. Figure 75 shows an OS1063 system equipped with two 21-port E1 modules for a total of 63 E1 ports.

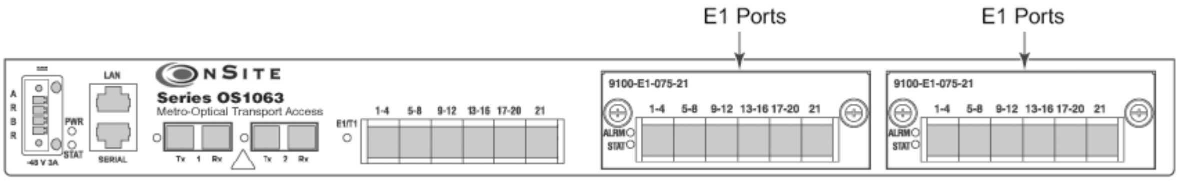


Figure 75. OS1063 with two 21-port E1 Expansion Modules

Table 51 provides the interconnection parameters for the E1 and T1 port options for the base system.

Table 51. E1 and T1 Port Interconnection Parameters

Parameter	E1 Ports	T1 Ports
Connector	Future Bus	Future Bus
Termination	120-ohm (balanced) or 75-ohm (unbalanced)	100-ohm, balanced
Line code	HDB3	AMI or B8ZS
Interconnecting cable	Category 3 or 5	Category 3 or 5
Reach	Short-haul	655 feet

Note The OS1052 and OS1063 support E1 signals with direct 120-ohm or 75-ohm termination as a factory-installed option.

The OS-10 uses a high-density Future Bus connector for access to the E1 ports. The connector is divided into six sections. Each section supports bidirectional transmission of four E1 ports. Connector section 6, however, supports only one E1 port for a combined total of 21 E1 ports.

WARNING **The E1 and T1 ports are non-telecommunications network voltage (TNV) and are for indoor use only. A CSU/DSU (channel service unit/data service unit) is required for outside plant installations.**

E1 and T1 Provisioning

The following section provides the procedures for enabling and disabling E1 and T1 ports. It also provides the procedures for configuring the external synchronization input and output ports, and the connection of traffic from E1 and T1 ports to SDH. The section concludes with the procedures for monitoring alarms and performance data at the E1 and T1 levels and setting up the loopback test function for E1 and T1 signals.

Enabling a Port for Service

To configure an E1 or a T1 port for service, see Figure 76 and Figure 77 on page 150 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the E1 or T1 port being configured and click on **Properties**. The system displays all E1 or T1 ports in slot 1 of the base OS-10 system. It also displays all E1 ports in slot 2 and slot 3 if the system is equipped with E1 expansion modules.

> **Note** The system uses the following naming convention for E1 and T1 interfaces: E1:slot/port and T1:slot/port. For instance, E1:1/3 refers to the E1 port 3 in slot 1. The base OS1052 system contains 8 E1 ports in slot 1 (the base system); that is, E1:1/1 through E1:1/8. The base OS1063 system contains 21 E1 ports in slot 1; that is, E1:1/1 through E1:1/21. If the system has a 21-port E1 expansion module in slot 2, E1:2/18 would refer to E1 port 18 in slot 2.

4. In the **Port Properties** window (see Figure 77 on page 150), set **Admin Status** to **Enabled**.

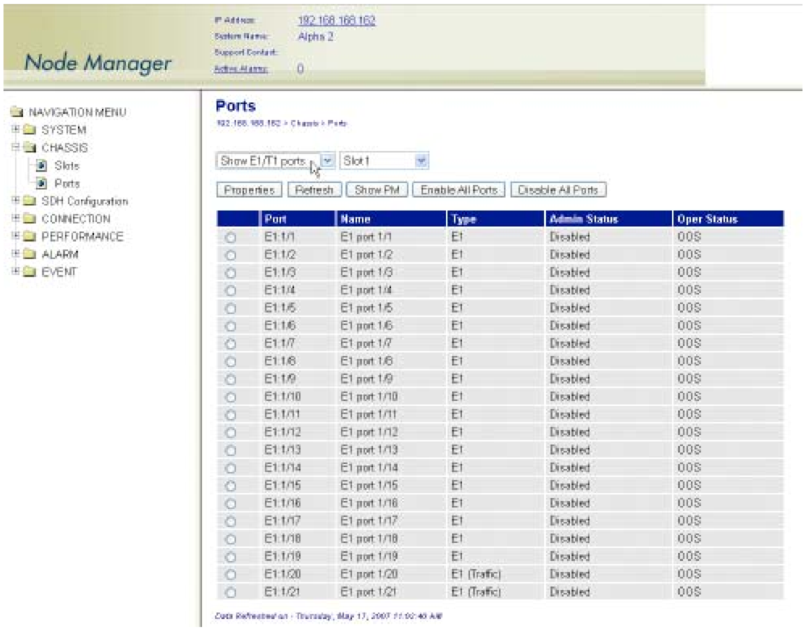
You can use the port selector filters at the top of the Ports page to narrow the selection of ports according to port type and location. By default, the filters are set to **Show all port types** in the **Base board**. To display, for instance, only the E1 ports in slot 2, use the scroll-down buttons to select **Show E1/T1 ports** and **Slot 2**. If you click on **Enable All Ports**, the system sets the **Admin Status** to **Enabled** for only the ports that are on display.

5. For systems that support the T1 port option, set the **Line Coding** to **B8ZS** (**default**) or **AMI**.

> **Note** For E1 ports, the line coding is always set to HDB3.

6. For systems that support the T1 port option, use the **Line Length** (**LBO meters**) scroll-down button to select the line-build out (LBO) settings for the T1 port.
7. Click on **Apply** and then on **Close** to close the window.

On the **Ports** page, **Admin Status** for the selected E1 or T1 port should now read **Enabled**.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

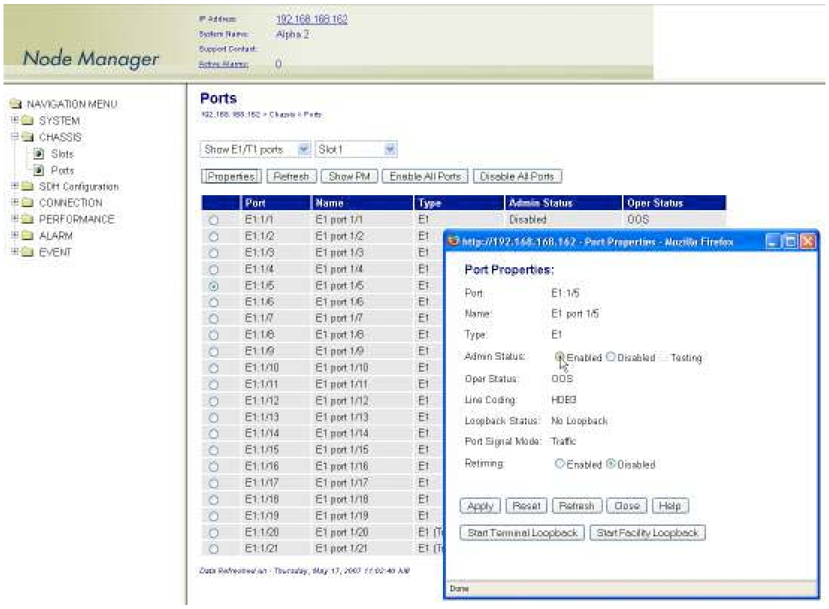
Ports

192.168.168.162 > Chassis > Ports

	Port	Name	Type	Admin Status	Oper Status
○	E1:1/1	E1 port 1/1	E1	Disabled	OOS
○	E1:1/2	E1 port 1/2	E1	Disabled	OOS
○	E1:1/3	E1 port 1/3	E1	Disabled	OOS
○	E1:1/4	E1 port 1/4	E1	Disabled	OOS
○	E1:1/5	E1 port 1/5	E1	Disabled	OOS
○	E1:1/6	E1 port 1/6	E1	Disabled	OOS
○	E1:1/7	E1 port 1/7	E1	Disabled	OOS
○	E1:1/8	E1 port 1/8	E1	Disabled	OOS
○	E1:1/9	E1 port 1/9	E1	Disabled	OOS
○	E1:1/10	E1 port 1/10	E1	Disabled	OOS
○	E1:1/11	E1 port 1/11	E1	Disabled	OOS
○	E1:1/12	E1 port 1/12	E1	Disabled	OOS
○	E1:1/13	E1 port 1/13	E1	Disabled	OOS
○	E1:1/14	E1 port 1/14	E1	Disabled	OOS
○	E1:1/15	E1 port 1/15	E1	Disabled	OOS
○	E1:1/16	E1 port 1/16	E1	Disabled	OOS
○	E1:1/17	E1 port 1/17	E1	Disabled	OOS
○	E1:1/18	E1 port 1/18	E1	Disabled	OOS
○	E1:1/19	E1 port 1/19	E1	Disabled	OOS
○	E1:1/20	E1 port 1/20	E1 (Traffic)	Disabled	OOS
○	E1:1/21	E1 port 1/21	E1 (Traffic)	Disabled	OOS

Data Refreshed on : Thursday, May 17, 2007 11:02:46 AM

Figure 76. Displaying E1 and T1 Ports



Port Properties:

Port: E1:1/5
Name: E1 port 1/5
Type: E1
Admin Status: ● Enabled ○ Disabled Testing
Oper Status: OOS
Line Coding: HDB3
Loopback Status: No Loopback
Port Signal Mode: Traffic
Retiming: ○ Enabled ● Disabled

Figure 77. Enabling an E1 or a T1 Port

Note The operational status (Oper Status) for an E1 or a T1 port is IS (in service) when the port Admin Status is Enabled and no alarms are present. Otherwise, the Oper Status for the port indicates OOS (out of service).

Disabling a Port from Service

To disable an E1 or a T1 port from service, follow these steps:

1. In the **Port Properties** window, set **Admin Status** to **Disabled**.
2. Click on **Apply** and then on **Close** to close the window.

On the **Ports** page, **Admin Status** for the selected E1 or T1 port should now read **Disabled**.

Note When an E1 or a T1 port is disabled, no port-related alarms are reported. PM data collection is also suspended. Furthermore, the system turns off the transmitter on the outgoing E1 or T1 signal. The system inserts E1 AIS into the VC-12 or T1 AIS into the VC-11 when an E1 or a T1 port is disabled, but remains connected to a TU-12 time slot.

Configuring a Port for Synchronization

The Port Properties windows for E1 ports 7 and 8 in slot 1 of the OS1052 (that is, E1:1/7 and E1:1/8) are different from other E1 ports in the base OS1052 system. Likewise, E1 ports 20 and 21 in slot 1 of the OS1063 (that is, E1:1/20 and E1:1/21) are different from other E1 ports in the base OS1063 system. These ports can be configured in one of three modes, as shown in Table 52.

Table 52. Configuration Modes for E1 Ports 7 and 8 (OS1052) and 20 and 21 (OS1063

Mode	The Port . . .
Traffic	Carries regular E1 traffic (default mode) and can be used for E1 line timing
Sync In	Serves as an external timing input for synchronizing the OS-10 system
Sync Out	Serves as an external timing output for synchronizing other equipment

To configure E1:1/7 and E1:1/8 in the OS1052 (or E1:1/20 and E1:1/21 in the OS1063) for synchronization purposes, see Figure 78 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select E1:1/7 in the OS1052 (or E1:1/20 in the OS1063) and click on **Properties**.
4. In the **Port Properties** window, set **Port Signal Mode** to one of the following: **Sync In**, **Sync Out** or **Traffic**.

Note By default, **Port Signal Mode** for **E1:1/7** and **E1:1/8** in the OS1052 (or E1:1/20 and E1:1/21 in the OS1063) is set to **Traffic**. In this mode, the system is synchronized using the derived clock from these ports when the timing mode is set to Auto: E1 port 7, port 8 in the OS1052 or **Auto: E1 port 20, port 21** in the OS1063. The system allows the connection of E1 traffic between these ports and TU-12 time slots on the STM-1 port when the ports are set as **Traffic**.

Note The system does not allow the connection of E1 traffic between these ports and TU-12 time slots on the STM-1 port when the ports are set as Sync In or Sync Out. Conversely, if either port is already connected to a TU-12 time slot, the system does not allow setting the port as Sync In or Sync Out.

Note The OS1052 does not allow the configuration of E1 port 7 or port 8 to Sync Out if the system timing mode is set to **Auto: E1 port 7, port 8**. Likewise, the OS1063 does not allow the configuration of E1 port 20 or port 21 to Sync Out if the system timing mode is set to **Auto: E1 port 20, port 2**.

5. Click on **Apply** and then on **Close** to close the window.

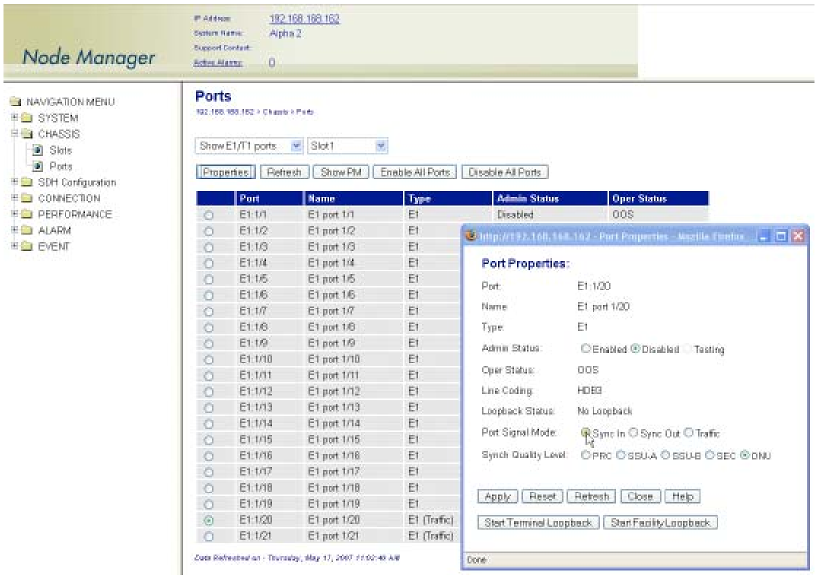
On the **Ports** page, the **Type** field for **E1:1/7** and **E1:1/8** in the OS1052 (or E1:1/20 and E1:1/21 in the OS1063) reflects the current **Port Signal Mode** setting.

To configure the synchronization quality level of an E1 Sync In port, see Figure 78 and follow these steps:

1. In the **Port Properties** window for E1 port 7 and 8 in the OS1052 (or E1 port 20 and 21 in the OS1063), set the **Sync Quality Level** to one of the following options (**PRC, SSU-A, SSU-B, SEC** or **DNU**).

Note The default setting is DNU. The quality level should be set in accordance with the timing source that generates the E1 Sync In signals.

2. Click on **Apply** and then on **Close** to close the window.



	Port	Name	Type	Admin Status	Oper Status
○	E1:1/1	E1 port 1/1	E1	Disabled	OOS
○	E1:1/2	E1 port 1/2	E1		
○	E1:1/3	E1 port 1/3	E1		
○	E1:1/4	E1 port 1/4	E1		
○	E1:1/5	E1 port 1/5	E1		
○	E1:1/6	E1 port 1/6	E1		
○	E1:1/7	E1 port 1/7	E1		
○	E1:1/8	E1 port 1/8	E1		
○	E1:1/9	E1 port 1/9	E1		
○	E1:1/10	E1 port 1/10	E1		
○	E1:1/11	E1 port 1/11	E1		
○	E1:1/12	E1 port 1/12	E1		
○	E1:1/13	E1 port 1/13	E1		
○	E1:1/14	E1 port 1/14	E1		
○	E1:1/15	E1 port 1/15	E1		
○	E1:1/16	E1 port 1/18	E1		
○	E1:1/17	E1 port 1/17	E1		
○	E1:1/18	E1 port 1/18	E1		
○	E1:1/19	E1 port 1/19	E1		
●	E1:1/20	E1 port 1/20	E1 (Trafic)		
○	E1:1/21	E1 port 1/21	E1 (Trafic)		

Data Refreshed on : Thursday, May 17, 2007 11:02:48 AM

Port Properties:

Port: E1:1/20
Name: E1 port 1/20
Type: E1
Admin Status: ○ Enabled ● Disabled ○ Testing
Oper Status: OOS
Line Coding: HDB3
Loopback Status: No Loopback
Port Signal Mode: ● Sync In ○ Sync Out ○ Trafic
Synch Quality Level: ○ PRC ○ SSU-A ○ SSU-B ○ SEC ● DNU

Figure 78. Configuring the Sync In and Sync Out Options

Retiming Mode

The base OS1052 and OS1063 systems support a retiming function for E1 ports 1-8 in slot 1, individually. In the regular mode of operation, the system uses the recovered clock from the demapped E1 signal for transmission into the physical E1 line. In the retiming mode, however, the system uses the system clock to transmit the E1 signal. You may use the retiming mode to distribute system timing to other equipment (such as PBXs or BTSs) that connects to the OS-10 at the E1 line level.

To enable the retiming feature for E1 ports in slot 1, see Figure 77 on page 150 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select **E1:1/*port*** and click on **Properties**.

Note The retiming function is available only for E1 port numbers 1-8, individually.

4. In the **Port Properties** window, set **Retiming** to **Enabled**.
5. Click on **Apply** and then on **Close** to close the window.

E1 and T1 Connections

The following section describes the process of setting up and removing connections between E1 and T1 ports and SDH TU-12 time slots using asynchronous mapping into VC-12 and VC-11 termination points.

The system maps T1 signals into VC-11 containers and adds a fixed stuff column with even parity to transport the VC-11 within a selected TU-12 time slot. This process is called “VC-11 to VC-12 conversion for transport over a TU-12” and is specified in ITU-T G.707. The system identifies this VC-11 as a VC-12 termination point for connection and management purposes.

Creating a Port Connection

To connect an E1 or a T1 port to a TU-12, see Figure 79 on page 155and follow these steps:

1. Select the **CONNECTION** folder from the navigation menu.
2. From the expanded **CONNECTION** folder, select **Client Port Mappings**.

If no connections are present, the table on the **Client Port Mappings** page is empty.

3. On the **Client Port Mappings** page, use the **Create Mapping Options...** scroll-down button to select the **Create E1/T1 Mapping** option.
4. In the **Create E1/T1 Mapping** window, select the E1 or T1 port to be connected using the **E1/T1 port** scroll-down button.

The system allows the creation of several E1 and T1 port connections at a time. To select more than one E1 or T1 port from the **E1/T1 port** list, click on individual entries while pressing the Ctrl key. (The system highlights any entry that you select from the list. You can select any entry from the list, whether the E1 or T1 ports are contiguous or not.)

To select a range of consecutive entries from the list, select the first entry and then select the last entry while pressing the Shift key.

Use the **Reset** button to restore the window to the default selection.

> **Note** The scroll-down list displays only the E1 and T1 ports that remain unconnected to TU-12s. The system displays and allows the connection of disabled E1 and T1 ports to TU-12s. An E1 or a T1 port connected to a TU-12 sends AIS over the VC-12 TP when the port is disabled.

You may enable (or disable) an E1 or a T1 port to activate (or deactivate) E1 or T1 service without deleting an existing connection. By connecting an E1 or a T1 port to a TU-12 and leaving the E1 or T1 port as disabled, you may test the connectivity and performance of the VC-12 path across the SDH network before allowing customer traffic from the E1 port to pass across the STM-1 interface.

5. Select the STM-1 port where you wish to connect the E1 or T1 port, using the **STM-1 port** scroll-down button.

The system presents a list of all available STM-1 ports in the system, including STM-1 ports in expansion slots 2 and 3, if present. The system also indicates the **Protection Type** for the selected port: Linear 1+1 MSP or SNCP.

6. Select the TU-12 to which the E1 or T1 port is to be connected using the **TU-12 Location** scrolldown button.

The scroll-down list system displays only the TU-12 time slots that remain unconnected in the selected STM-1 port.

> **Note** The **TU-12 Location** for the TU-12 is indicated by the SDH indexing scheme (ST:1/1-U/K/L/M. The system displays the default **TU-12 Location** associated with the selected E1 or T1 port. However, you can select any available TU-12 on the list.

> **Note** By default, the system displays the TU-12 timeslots in logical sequence order. To display the timeslots in physical order, set **TU Sequencing Type** to **Physical order**.

To select more than one **TU-12 location** from the TU-12 Location list, click on individual entries while pressing the Ctrl key. (The system highlights any entry that you select from the list. You can select any entry from the list, whether the TU-12 locations are contiguous or not.)

To select a range of consecutive entries from the list, select the first entry and then select the last entry while pressing the Shift key.

Use the **Reset** button to restore the window to the default selection.

> **Note** Make sure that the number of selected entries from the list matches the number of selected E1 ports in the **E1/T1 port** list before proceeding; otherwise, the system rejects the creation of the connections.

7. If you wish to connect the E1 or T1 port to the TU-12 as a 2-way (bidirectional) connection, leave **Direction** as **2-way**.

However, for 1-way (unidirectional) connections, set **Direction** to **1-way**, and set the **Connection Point** button for **TU-12 Location** to indicate whether the TU-12 is the **Sink** or **Source** point for the connection.

For drop-and continue connections, set **Direction** to either **1-way drop-continue** or **2-way drop-continue**.

For multicast connections, set **Direction** to **1-way multicast**.

If you plan to drop E1 or T1 traffic from a single TU-12 into more than one E1 or T1 port in the same system slot, you must first start with the creation of a single 1-way multicast connection (and not with a regular 1-way connection) between the source TU-12 and the first of the E1 or T1 sink ports. Once the first multicast connection is present, you can add other multicast connection legs between the same TU-12 and other sink ports in the slot.

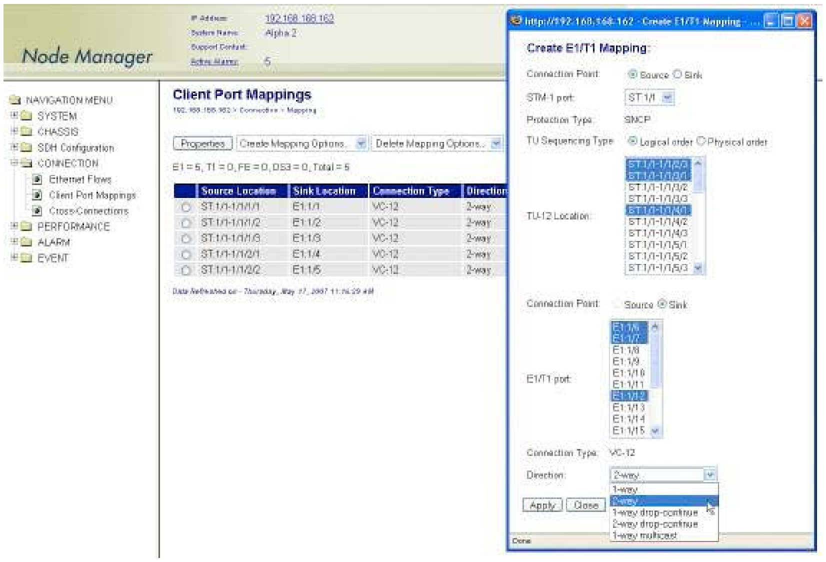
Note For Drop-and-continue and multicast connections, the system requires that the TU-12 is the source point of the connection.

8. Click on **Apply** to initiate the creation of the E1 or T1 connections.

CAUTION

The **Create E1/T1 Mapping** window closes automatically after the system completes the creation of the E1 or T1 connections. If the number of connections is large, the system may take a few seconds to create the connections and close the window. Closing the window manually before.the process is complete may cause an error or partial creation of the new connections. Click on **Refresh** on the **Client Port Mappings** page to update the table with the new connections after the window closes.

Note The system does not allow the connection of E1 port 7 or port 8 in slot 1 of the OS1052 (or E1 port 20 or port 21 in slot 1 of the OS1063) to a TU-12 time slot if the port is configured in Sync In or Sync Out mode.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 5

Client Port Mappings

192.168.168.162 > Connection > Mapping

E1 = 5, T1 = 0, FE = 0, DS3 = 0, Total = 5

	Source Location	Sink Location	Connection Type	Direction
○	ST1/1-1/1/1/1	E1:1/1	VC-12	2-way
○	ST1/1-1/1/1/2	E1:1/2	VC-12	2-way
○	ST1/1-1/1/1/3	E1:1/3	VC-12	2-way
○	ST1/1-1/1/2/1	E1:1/4	VC-12	2-way
○	ST1/1-1/1/2/2	E1:1/5	VC-12	2-way

Data Refreshed on - Thursday, May 17, 2007 11:16:29 AM

Create E1/T1 Mapping:

Connection Point: ● Source ○ Sink

STM-1 port: ST 1/1

Protection Type: SNCP

TU Sequencing Type: ● Logical order ○ Physical order

TU-12 Location: ST1/1-1/1/2/3, ST1/1-1/1/3/1, ST1/1-1/1/3/2, ST1/1-1/1/3/3, ST1/1-1/1/4/1, ST1/1-1/1/4/2, ST1/1-1/1/4/3, ST1/1-1/1/5/1, ST1/1-1/1/5/2, ST1/1-1/1/5/3

Connection Point: ○ Source ● Sink

E1/T1 port: E1:1/6, E1:1/7, E1:1/8, E1:1/9, E1:1/10, E1:1/11, E1:1/12, E1:1/13, E1:1/14, E1:1/15

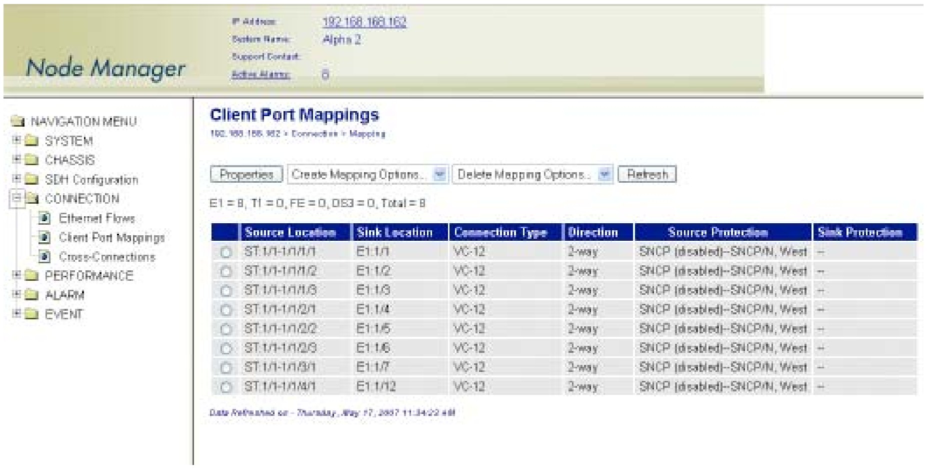
Connection Type: VC-12

Direction: 2-way (1-way, 2-way, 1-way drop-continue, 2-way drop-continue, 1-way multicast)

Figure 79. Connecting an E1 or a T1 port to a TU-12

The **Client Port Mappings** table now displays the newly made connections (see Figure 80).

> **Note** The system enables the VC-12 TP into which the E1 or T1 signal is mapped only after the connection is made. Only at this point the TU-12 time slot that carries the VC-12 TP no longer sends the unequipped signal.



Client Port Mappings

192.168.168.162 > Connection > Mapping

E1 = 8, T1 = 0, FE = 0, DS3 = 0, Total = 8

	Source Location	Sink Location	Connection Type	Direction	Source Protection	Sink Protection
○	ST:1/1-1/1/1/1	E1:1/1	VC-12	2-way	SNCP (disabled)--SNCP/N, West	--
○	ST:1/1-1/1/1/2	E1:1/2	VC-12	2-way	SNCP (disabled)--SNCP/N, West	--
○	ST:1/1-1/1/1/3	E1:1/3	VC-12	2-way	SNCP (disabled)--SNCP/N, West	--
○	ST:1/1-1/1/2/1	E1:1/4	VC-12	2-way	SNCP (disabled)--SNCP/N, West	--
○	ST:1/1-1/1/2/2	E1:1/5	VC-12	2-way	SNCP (disabled)--SNCP/N, West	--
○	ST:1/1-1/1/2/3	E1:1/6	VC-12	2-way	SNCP (disabled)--SNCP/N, West	--
○	ST:1/1-1/1/3/1	E1:1/7	VC-12	2-way	SNCP (disabled)--SNCP/N, West	--
○	ST:1/1-1/1/4/1	E1:1/12	VC-12	2-way	SNCP (disabled)--SNCP/N, West	--

Data Refreshed on - Thursday, May 17, 2007 11:34:22 AM

Figure 80. Displaying E1 and T1 connections

Configuring the SNCP Protection Options for E1/T1 Connections

By default, E1 or T1 connections to an SNCP-ready STM-1 port are unprotected. As shown in Figure 81, for unprotected connections, both directions of transmission are connected to STM-1 port 1 (west port) or port 2 (east port).

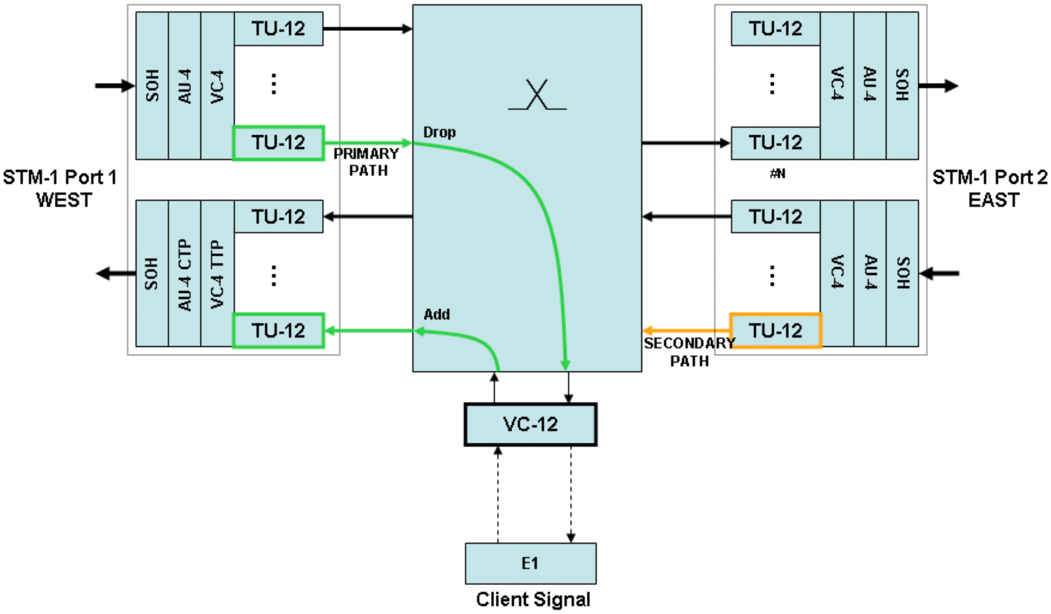


Figure 81. Unprotected E1 or T1 Connections

If an E1 or T1 port is connected to an STM-1 port that supports SNCP protection, you can protect the connection end point using SNCP/I or SNCP/N. When SNCP is enabled, the system activitates the bridging and path selector functions for the connection, as shown in Figure 66 on page 133.

To protect an existing E1 or T1 connection using SNCP, see Figure 80 on page 156 and Figure 82, and follow these steps:

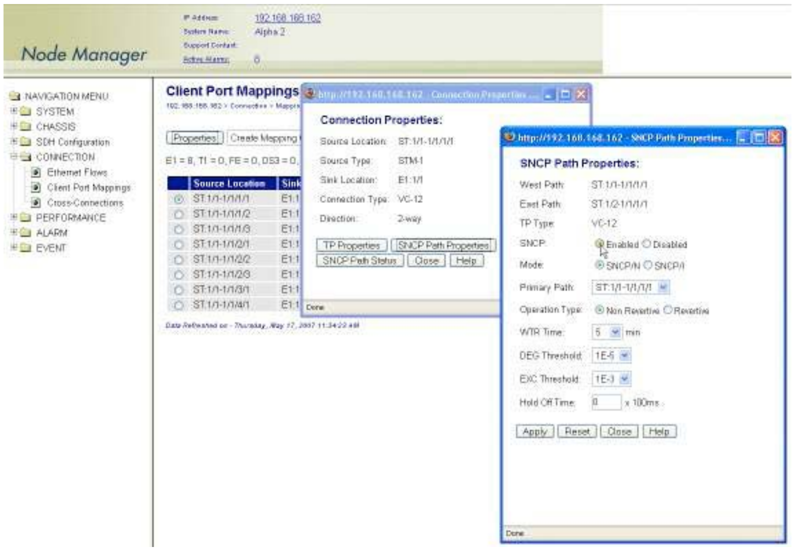
1. On the **Client Port Mappings** page, select the table entry that contains the E1 or T1 connection that you wish to protect and click on Properties.
2. In the **Connection Properties** window, click on **SNCP Path Properties.**
3. In the **SNCP Path Properties** window, set **SNCP** to **Enabled**.

Note SNCP can be enabled only if the E1/T1 port is connected to STM-1 port 1 (west port).

At this time, you may change other SNCP path properties, including the **Mode** (SNCP/I or SNCP/N), **Operation Type** (non-revertive or revertive) and **Hold Off Time**. If the **Mode** is set to SNCP/N, you may also change the **DEG Threshold** and **EXC Threshold**. (In SNCP/I mode, the system does not use the DEG and EXC thresholds to initiate the protection switch.) See Table 54 for the definitions of the SNCP path properties. At this time you may also change the **Primary Path** from STM-1 port 1 (west port) to STM-1 port 2 (east port).

Note By default, the primary path in an SNCP connection is located on the west port. The primary and secondary paths are symmetrical. That is, both paths have the same TU-12 time slot index (U/K/L/M) on the east and west STM-1 ports.

4. Click on **Apply** and **Close** the **SNCP Path Properties** window.
5. **Close** the Connection Properties window.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

Client Port Mappings
192.168.168.162 > Connection > Mappi

E1 = 8, T1 = 0, FE = 0, DS3 = 0,

	Source Location	Sink
●	ST:1/1-1/1/1/1	E1:1
○	ST:1/1-1/1/1/2	E1:1
○	ST:1/1-1/1/1/3	E1:1
○	ST:1/1-1/1/2/1	E1:1
○	ST:1/1-1/1/2/2	E1:1
○	ST:1/1-1/1/2/3	E1:1
○	ST:1/1-1/1/3/1	E1:1
○	ST:1/1-1/1/4/1	E1:1

Data Refreshed on - Thursday, May 17, 2007 11:34:22 AM

http://192.168.168.162 - Connection Properties ...

Connection Properties:

Source Location: ST:1/1-1/1/1/1
Source Type: STM-1
Sink Location: E1:1/1
Connection Type: VC-12
Direction: 2-way

http://192.168.168.162 - SNCP Path Properties...

SNCP Path Properties:

West Path: ST:1/1-1/1/1/1
East Path: ST:1/2-1/1/1/1
TP Type: VC-12
SNCP: ● Enabled ○ Disabled
Mode: ● SNCP/N ○ SNCP/I
Primary Path: ST:1/1-1/1/1/1
Operation Type: ● Non Revertive ○ Revertive
WTR Time: 5 min
DEG Threshold: 1E-5
EXC Threshold: 1E-3
Hold Off Time: 0 x 100ms

Figure 82. Protecting E1 and T1 Connections Using SNCP

Configuring the J2 Trace

To configure the J2 trace message for the VC-12 TP that carries the E1 or T1 signal, see Figure 83 and follow these steps.

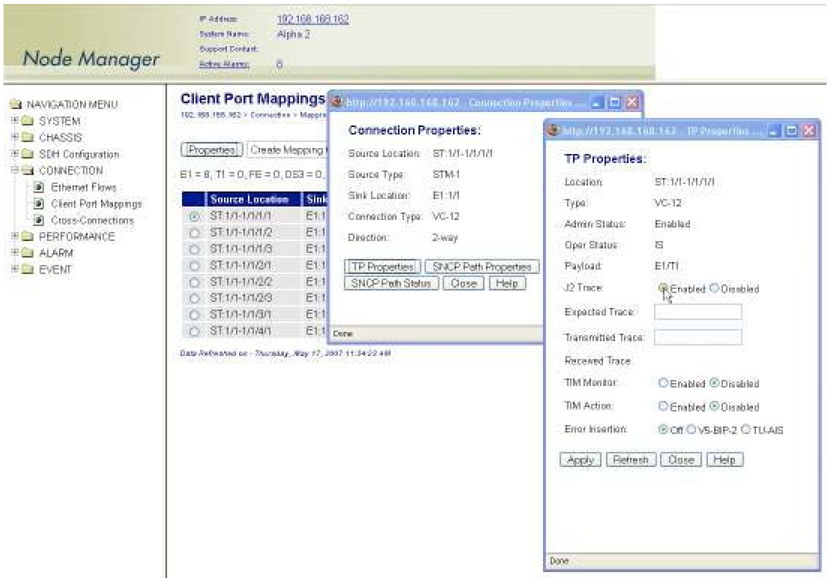
1. In the **Client Port Mappings** page, select the table entry for the required E1 or T1 connection and click on **Properties**.
2. In the **Connection Properties** window, click on **TP Properties**.
3. In the **TP Properties** window, set the **J2 Trace** to **Enabled**.
   - – Set **TIM Monitor** to **Enabled**, if you wish to detect trace identifier mismatch (TIM) defects for the VC-12 TP using the J2 trace.
   - – Set **TIM Action** to **Enabled**, if you wish to generate a consequent action (AIS downstream and LP-RDI upstream) upon detection of a TIM defect for the VC-12 TP using the J2 trace.
4. Type the **Expected Trace** and the **Transmitted Trace** using up to 15 ASCII characters for each field.

> **Note** The system inserts the transmitted trace into the outgoing J2 byte for the selected VC-12 TP.

5. Click on **Apply** and then on **Close** to close the **TP Properties** window.

> **Note** The system does not allow enabling the J2 trace with the expected trace and transmitted trace fields empty. The system displays the **Received Trace** message if any is being received from the incoming J2 byte for the selected VC-12 TP.

6. Click on **Close** to close the Connection Properties window.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

Client Port Mappings

192.168.168.162 > Connection > Mappi

E1 = 8, T1 = 0, FE = 0, DS3 = 0,

	Source Location	Sink
●	ST:1/1-1/1/1/1	E1:1
○	ST:1/1-1/1/1/2	E1:1
○	ST:1/1-1/1/1/3	E1:1
○	ST:1/1-1/1/2/1	E1:1
○	ST:1/1-1/1/2/2	E1:1
○	ST:1/1-1/1/2/3	E1:1
○	ST:1/1-1/1/3/1	E1:1
○	ST:1/1-1/1/4/1	E1:1

Data Refreshed on - Thursday, May 17, 2007 11:34:22 AM

http://192.168.168.162 - Connection Properties ...

Connection Properties:

Source Location: ST:1/1-1/1/1/1
Source Type: STM-1
Sink Location: E1:1/1
Connection Type: VC-12
Direction: 2-way

http://192.168.168.162 - TP Properties ...

TP Properties:

Location: ST:1/1-1/1/1/1
Type: VC-12
Admin Status: Enabled
Oper Status: IS
Payload: E1/T1
J2 Trace: ● Enabled ○ Disabled
Expected Trace:
Transmitted Trace:
Received Trace:
TIM Monitor: ○ Enabled ● Disabled
TIM Action: ○ Enabled ● Disabled
Error Insertion: ● Off ○ VS-BIP-2 ○ TU-AIS

Figure 83. Configuring the J2 Trace

You can also configure the TP properties for all existing VC-12 TPs in the system by following these steps.

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select **Termination Points**.
3. On the **Termination Points** page, select the table entry for the VC-12 TP that you wish to configure and click on **Properties**.
4. On the **TP Properties** window, you may know configure the J2 trace and the Error Insertion features for the selected VC-12 TP.
5. Click on **Close** to close the TP Properties window.

Removing a Port Connection

To remove an existing E1 or T1 port-to-TU-12 connection, follow these steps:

1. Select an E1 or a T1 port connection on the **Client Port Mappings** page.
2. Click on **Delete** to remove the port connection.

At this point, the system removes the connection and it is no longer displayed in the table.

Note The system automatically disables the VC-12 TP after deletion of the connection to the TU-12 time slot. At this point, the system starts to send the unequipped signal over this TU-12. The time slot is now available for other connections.

E1 and T1 Alarms

The following section describes the process for monitoring alarms that may be present on E1 and T1 ports and the process of changing the default alarm settings.

Monitoring Port Alarms

Table 53 provides a list of the alarms that the system monitors at the E1 and T1 line level.

Table 53. E1 and T1 Line Alarms

Alarm	Description	Definition
PDH LOS	Loss of Signal	Incoming signal has no transitions for *n* consecutive pulse intervals

Note The system declares and displays an alarm condition if a defect persists for 2.5 ± 0.5 seconds. The alarm condition is cleared when the defect is terminated and remains absent for 10 ± 0.5 seconds.

The front panel provides an alarm status LED to indicate the presence of an active alarm condition of any severity level (Critical, Major, Minor, or Warning) on any of the eight E1 or eight T1 ports on the base OS-10 system. The LED is lit according to the color codes in Table 54 on page 160.

Table 54. E1 or T1 Alarm Status LED

LED Color	Description
Green	No alarm is present on any port.
Amber	An alarm is present on one or more ports.
Off	All E1 or T1 ports are disabled.

To display E1 and T1 alarms, if present, see Figure 84 and follow these steps:

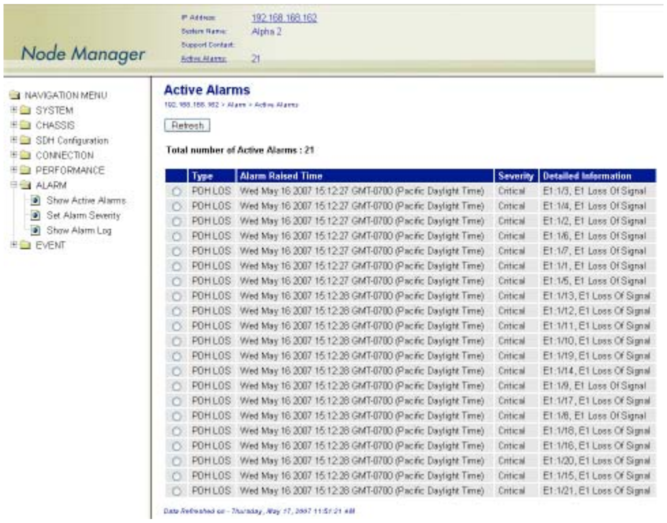
1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Show Active Alarms**.

At this point, the **Active Alarms** page displays all active alarms in the system, including E1 and T1 alarms, if present. The table contains a separate entry for each active alarm. Table 55 describes the fields for each E1 and T1 alarm entry.

Table 55. Table Entries for Active E1 and T1 Alarms

Table Entry for Active Alarms	Field Value
Type	**PDH LOS, Loopback**
Alarm Raised Time	Date and time
Severity	Critical, Major, Minor, or Warning
Detailed Information	Location of affected E1 or T1 port (E1:*slot/port* or T1:*slot/port*)

Note The system automatically updates the Active Alarms page every 60 seconds. Click on Refresh if you need to update the table with the most recent active alarm information. Individual table entries automatically clear whenever previously active alarms are no longer present.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 21

Active Alarms

192.168.168.162 > Alarm > Active Alarms

Total number of Active Alarms : 21

	Type	Alarm Raised Time	Severity	Detailed Information
○	PDH LOS	Wed May 16 2007 15:12:27 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/3, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:27 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/4, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:27 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/2, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:27 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/6, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:27 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/7, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:27 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/1, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:27 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/5, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/13, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/12, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/11, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/10, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/19, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/14, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/9, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/17, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/8, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/18, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/16, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/20, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/15, E1 Loss Of Signal
○	PDH LOS	Wed May 16 2007 15:12:28 GMT-0700 (Pacific Daylight Time)	Critical	E1:1/21, E1 Loss Of Signal

Data Refreshed on - Thursday, May 17, 2007 11:51:21 AM

Figure 84. Displaying E1 and T1 Port Alarms

Changing Port Alarm Default Severities

Table 56 provides the default severities for E1 and T1 line alarms:

Table 56. E1 and T1 Line Alarm Default Severities

Monitored Entity	Near-end Alarm	Default Severity
E1 or T1 port	PDH LOS	Critical

To change the default severity for supported E1 and T1 alarms, follow these steps:

1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Set Alarm Severity**.

At this point, the **Alarm Severity** page displays a table with all supported system alarms.

3. Select the table entry containing the E1 or T1 port alarm **Type** (**PDH LOS**) and click on **Change**.
4. In the **Alarm Severity** window, set **Severity** to any desired level (**Critical, Major, Minor,** or **Warning**).
5. Click on **Apply** and then on **Close** to close the window.

On the **Alarm Severity** page, the Severity for the selected E1 or T1 port alarm **Type** should now reflect the change in the reported severity level.

Note The change applies to all E1 and T1 ports within the system.

Displaying the Alarm Log

To display historical alarms, including any E1 or T1 port alarms if present, follow these steps:

1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Show Alarm Log**.

At this point, the **Alarm Log** page displays a list of the 50 most recent alarm messages. The system keeps up to 500 entries in the alarm log.

Note The alarm log is a FIFO (first-in fist-out) log.

Click on **Last 50 Log Entries** or **Next 50 Log Entries** to move around and display the entire contents of the log. Click on **Clear Log** if you wish to delete permanently the current log entries.

E1 and T1 Performance Monitoring

The following section describes the process for displaying current and historical PM data for E1 and T1 ports.

Monitoring E1 and T1 Port Performance

Table 57 provides a list of the E1 and T1 Line PM parameters (near-end) that the system monitors in accordance with G.826.

Table 57. E1 and T1 Line PM Parameters

Parameter	Description	Definition
LCV	Line Coding Violation	Count of BPV or EXZ over the accumulation period
ES	Errored Second	Count of seconds in which the LCV count is greater than or equal to 1 or in which a LOS defect occurs
SES	Severely Errored Second	Count of seconds in which the LCV count is greater than or equal to 2048 for E1 signals (1544 for T1 signals) or in which a LOS defect occurs
UAS	Unavailable Seconds	Period of unavailable time that begins at the onset of 10 consecutive SES

To display current PM data for an E1 or a T1 port, see Figure 85 on page 163 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the E1 or T1 port being configured and click on **Show PM**.

At this point, the **E1/T1 Near-end PM** page shows the near-end PM data for both the current 15-minute and 24-hour periods.

Note The PM data is not updated automatically as new events occur during the current 15-minute and 24-hour periods. Click on **Refresh** to update the tables with the most recent cumulative count for the current periods.

Continue with the steps that follow to display historical PM data.

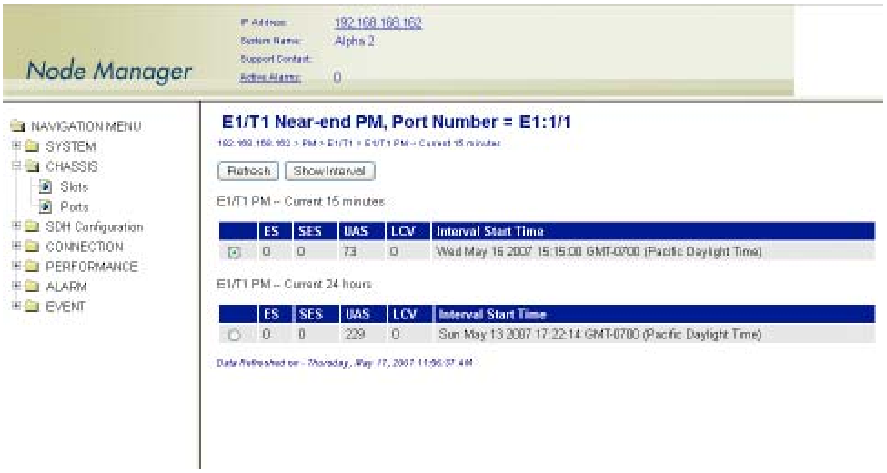
4. Click on **Show Interval**.

At this point, the **E1/T1 Near-end PM** page shows the near-end PM data for the following intervals:

- Current plus previous 95-by-15-minute intervals (24 hours total)
- Current plus previous day (2 days total)

Click on **Refresh** to update the tables with the most recent cumulative count for the current periods. This action updates only the first entry in the tables, which corresponds to the current measurement period.

Note The tables display **Invalid** under **PM data** when the data collected during a measurement period is considered invalid. The **Interval Start Time** also displays n/a (not available).



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

E1/T1 Near-end PM, Port Number = E1:1/1

192.168.168.162 > PM > E1/T1 > E1/T1 PM – Current 15 minutes

E1/T1 PM – Current 15 minutes

	ES	SES	UAS	LCV	Interval Start Time
◉	0	0	73	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)

E1/T1 PM – Current 24 hours

	ES	SES	UAS	LCV	Interval Start Time
○	0	0	229	0	Sun May 13 2007 17:22:14 GMT-0700 (Pacific Daylight Time)

Data Refreshed on - Thursday, May 17, 2007 11:56:37 AM

Figure 85. Displaying Current PM Data for E1 and T1 Ports

To display current and historical PM data for all E1 and T1 ports in the system, see Figure 86 on page 164 and follow these steps:

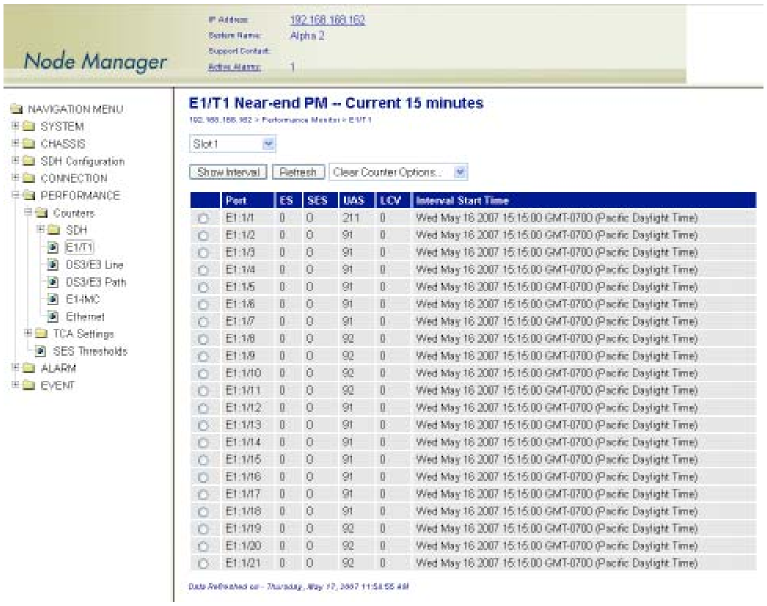
1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select **Counters**.
3. From the expanded **Counters** folder, select **E1/T1**.

At this point, the **E1/T1 Near-end PM** page shows the near-end PM data for the current 15-minute period only. The table displays PM data for only enabled E1/T1 ports. (The table entries are empty if no E1/T1 ports are enabled.)

Continue with the steps that follow to display historical PM data for both 15-minute and 24-hour periods.

4. Select an E1 or a T1 port and click on **Show Interval**.

Note The preceding notes for the **E1/T1 Near-end PM** page also apply to this procedure.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 1

E1/T1 Near-end PM -- Current 15 minutes

192.168.168.162 > Performance Monitor > E1/T1

Slot 1

	Port	ES	SES	UAS	LCV	Interval Start Time
○	E1:1/1	0	0	211	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/2	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/3	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/4	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/5	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/6	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/7	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/8	0	0	92	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/9	0	0	92	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/10	0	0	92	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/11	0	0	92	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/12	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/13	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/14	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/15	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/16	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/17	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/18	0	0	91	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/19	0	0	92	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/20	0	0	92	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)
○	E1:1/21	0	0	92	0	Wed May 16 2007 15:15:00 GMT-0700 (Pacific Daylight Time)

Data Refreshed on - Thursday, May 17, 2007 11:54:55 AM

Figure 86. Displaying Current PM Data for All E1 and T1 Ports

To clear the current PM data for an E1 or a T1 port, see Figure 86 and follow this step:

1. On the **E1/T1 Near-end PM** page, select an E1 or a T1 port entry and use the **Clear Counter Options...** scroll-down button to select one of the available options for clearing the current 15-minute counter, 24-hour counter, or both.

Configuring E1 and T1 Port Threshold Crossing Alerts (TCA)

The system supports threshold registers for E1 and T1 port PM parameters. A TCA event is generated when a monitored event reaches or crosses the preset threshold value within a given measurement period (15 minutes or 24 hours).

To configure the system for reporting TCA events at the E1 or T1 port level, follow these steps:

Note By default, the reporting of TCA events for E1 and T1 ports is disabled.

1. Select the **EVENT** folder from the navigation menu.
2. From the expanded **EVENT** folder, select **Enable TCA Event**.
3. On the **TCA Event Disable / Enable** page, change **TCA Events** (**E1/T1**) to **On**.
4. Click on **Apply** to complete this task.

Note This is a global setting. Enabling the report of TCA events applies to all E1 and T1 ports on the system.

To configure the default TCA settings for E1 and T1 ports, follow these steps:

1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select the **TCA Settings** folder.
3. From the expanded **TCA Settings** folder, select the **E1/T1** folder.
4. From the expanded **E1/T1** folder, select **Default**.
5. On the **E1/T1 Default TCA Settings** page, select the table entry and click on **Change**.
6. In the **E1/T1 Default TCA Settings** window, change the default TCA settings for the E1 and T1 line ES, SES, UAS and LCV parameters (current and day periods) as required.

Note The system displays the factory default TCA settings when you first open this page. Afterwards, the system displays any recent configuration changes. The preferred method of restoring the original settings is to reenter the values manually.

7. Click on **Apply** and then on **Close** to close the E1/T1 Default TCA Settings window.

Note The default values apply to all E1 and T1 ports on the system.

To assign custom TCA values for each individual E1 or T1 port on the system, continue with Step 8; otherwise, Step 7 completes this task.

8. From the expanded **E1/T1** folder, select **Custom**.

At this point, the **E1/T1 TCA Settings** page displays the current TCA settings for each E1 and T1 port on the system. The table entry indicates **Default** if the default TCA value is in use for a given parameter or **Custom** (**value**) if the system uses any custom value other than the default.

9. On the **E1/T1 TCA Settings** page, select the E1 or T1 port that you wish to configure and click on **Change**.
10. In the **E1/T1 TCA Settings** window, select **Custom** for the TCA settings that you wish to customize and change the setting to any value within the allowable range.

Note You may change the TCA settings for more than one parameter at a time.

11. Click on **Apply** and then on **Close** to close the E1/T1 TCA Settings window.

At this point, the **E1/T1 TCA Settings** page reflects any recent configuration changes.

If you wish to change a TCA setting back to its default setting, select **Default** instead of **Custom** in Step 10.

E1 and T1 Testing

The following section provides the procedures for enabling and disabling loopback tests for E1 and T1 ports.

Configuring E1 and T1 Terminal Loopback

The OS-10 system supports terminal loopback for E1 and T1 ports. As shown in Figure 87, while the terminal loopback is active, the E1 or T1 signal is looped back towards the STM-1 interface just before transmission on the E1 or T1 physical interface. E1 or T1 AIS is also transmitted on the physical port. Terminal loopback allows the testing of the performance and connectivity for an E1 or a T1 service across the SDH network.

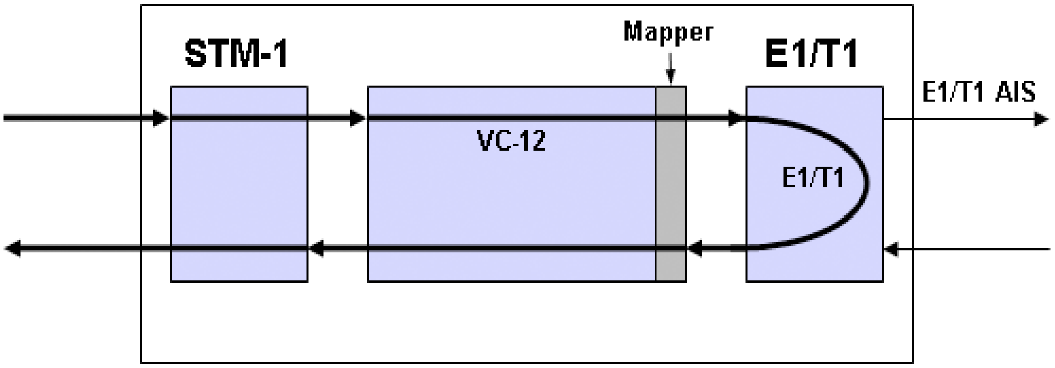


Figure 87. E1 and T1 Terminal Loopback

Configuring E1 and T1 Facility Loopback

The OS-10 system supports facility loopback for E1 and T1 ports, as shown in Figure 88. The loopback point occurs before mapping the E1 signal into a VC-12 or T1 signal into a VC-11. If a connection is already present, the system inserts E1 AIS into the VC-12 payload container (C-12) or T1 AIS into the VC-11 payload container (C-11) while the facility loopback is active. Facility loopback allows the testing of the performance and connectivity of the E1 or T1 cabling between the OS-10 system and the end-user equipment.

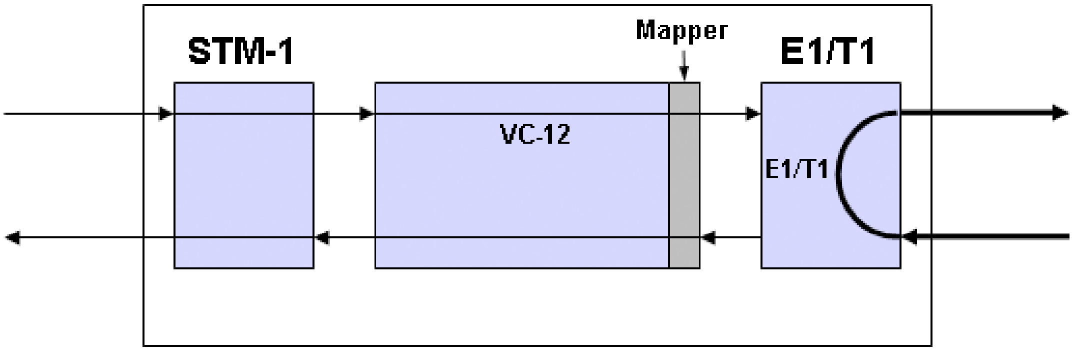


Figure 88. E1 and T1 Facility Loopback

To start an E1 or a T1 terminal loopback (or facility loopback) test, see Figure 89 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the E1 or T1 port being tested and click on **Properties**.
4. In the **Port Properties** window, click on **Start Terminal Loopback** or Start Facility Loopback.

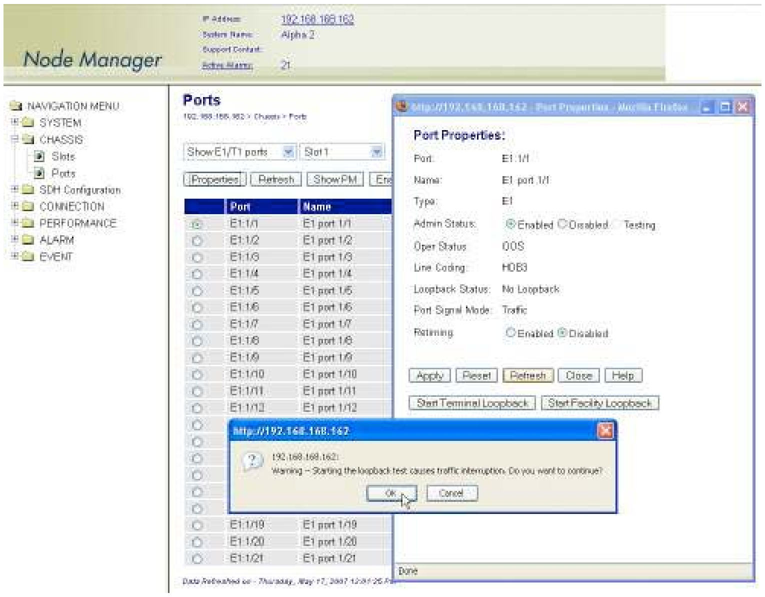
A warning window opens to alert you to the start of the loopback test. Click on **OK** to continue or **Cancel** to cancel the request.

WARNING

Starting an E1 or a T1 terminal loopback causes traffic disruption if the E1 or T1 port is already connected to a TU-12.

Loopback Status on the **Port Properties** window changes to **Terminal Loopback Active** or **Facility Loopback Active**. **Admin Status** for the port changes to **Testing**.

5. Click on **Close** to close the **Port Properties** window.



	Port	Name
●	E1:1/1	E1 port 1/1
○	E1:1/2	E1 port 1/2
○	E1:1/3	E1 port 1/3
○	E1:1/4	E1 port 1/4
○	E1:1/5	E1 port 1/5
○	E1:1/6	E1 port 1/6
○	E1:1/7	E1 port 1/7
○	E1:1/8	E1 port 1/8
○	E1:1/9	E1 port 1/9
○	E1:1/10	E1 port 1/10
○	E1:1/11	E1 port 1/11
○	E1:1/12	E1 port 1/12
○		
○		
○		
○		
○		
○		
○	E1:1/19	E1 port 1/19
○	E1:1/20	E1 port 1/20
○	E1:1/21	E1 port 1/21

Data Refreshed on - Thursday, May 17, 2007 12:31:25 PM

http://192.168.168.162 - Port Properties - Mozilla Firefox

Port Properties:

Port: E1:1/1
Name: E1 port 1/1
Type: E1
Admin Status: ● Enabled ○ Disabled ○ Testing
Oper Status: OOS
Line Coding: HDB3
Loopback Status: No Loopback
Port Signal Mode: Traffic
Retiming: ○ Enabled ● Disabled

192.168.168.162:
Warning -- Starting the loopback test causes traffic interruption. Do you want to continue?

Figure 89. Activating E1 Loopback

To stop an E1 or a T1 loopback test, follow these steps:

1. In the **Port Properties** window, set **Admin Status** to **Enabled** or **Disabled**, if required.
2. Click on **Apply**.

At this point, **Loopback Status** changes to **No Loopback**. The system resumes any connection previously present between the E1 or T1 port and a TU-12 time slot.

3. Click on **Close** to close the the **Port Properties** window.

Chapter 5 DS3/E3 Interface

Chapter contents

Introduction

This chapter provides the procedures for provisioning, monitoring, and testing of DS3 and E3 client signal ports using the 3-port DS3/E3 expansion module. Procedures for connecting DS3 and E3 traffic to SDH are also provided.

General Information

The DS3/E3 module has three (3) built-in DS3/E3 interface ports.

DS3/E3 traffic is mapped into a VC-3 using asynchronous mapping, as specified in ITU-T Recommendation G.707. The VC-3 is multiplexed into an STM-1 through the AU-4 multiplexing route, as shown in Figure 90.

Note Asynchronous mapping supports clear-channel transport of G.703 services at 44.736 Mbit/s ± 20 ppm for DS3 signals and at 34.368 Mbit/s ± 20 ppm for E3 signals.

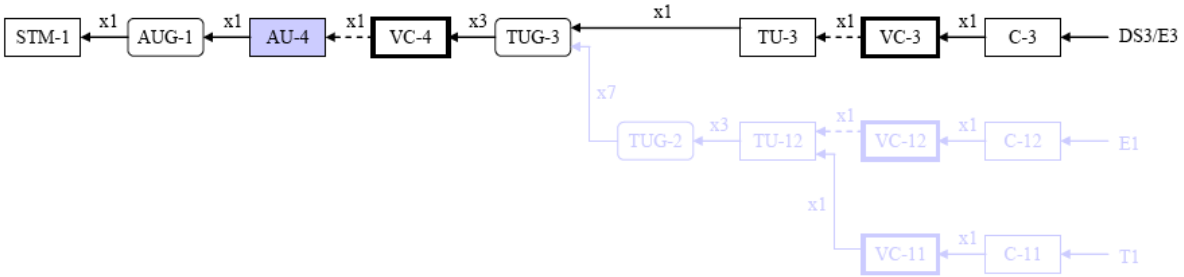


Figure 90. DS3 and E3 Multiplexing over SDH

The DS3 and E3 interfaces comply with the following standards:

- ITU-T G.703 and GR-449 (physical layer)
- ITU-T G.707 (SDH mapping)
- ITU-T G.775 and GR-499 (LOS detection)
- ITU-T G.826 and ANSI T1.231 (performance monitoring)
- ITU-T G.823, G.783, and GR-253 (jitter and wander)

For each DS3/E3 port, the module supports non-intrusive monitoring of path-level defects and the collection of performance-monitoring data in both directions of transmission (receive and transmit sides).

For ports configured as DS3, the system supports the following framing formats:

- M23
- C-bit parity
- Unframed

For ports configured as E3, the system supports the following framing formats:

- G.751
- G.832
- Unframed

The activation of the line framer does not disrupt or change the bit stream of the signal, even if the framer detects an incoming signal failure. (For example, the framer, if enabled, does not generate an AIS signal downstream upon detection of a loss-of-frame condition on the DS3 or E3 signal).

Figure 91 shows the location of the DS3 and E3 ports on the module.

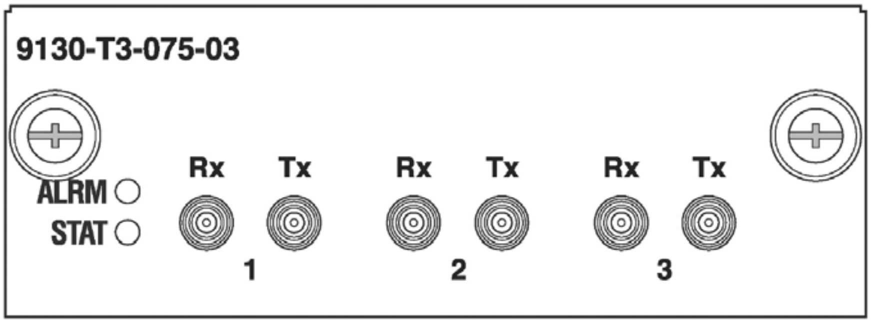


Figure 91. DS3 and E3 Ports on the 3-Port DS3/E3 Module

Table 58 provides the interconnection parameters for the DS3 and E3 port options.

Table 58. DS3 and E3 Port Interconnection Parameters

Parameter	DS3 Ports	E3 Ports
Connector	DIN 1.0/2.3	DIN 1.0/2.3
Termination	75-ohm, unbalanced	75-ohm, unbalanced
Line code	B3ZS	HDB3
Interconnecting cable	Coaxial cable	Coaxial cable
Reach	450 feet to DSX panel or 900 feet from transmit to receive	450 feet to DSX panel or 900 feet from transmit to receive

DS3 and E3 Provisioning

The following section provides the procedures for enabling and disabling DS3 and E3 ports. The section concludes with the procedures for monitoring alarms and performance data at the DS3 and E3 levels and setting up the loopback test function for DS3 and E3 signals.

Enabling a Port for Service

To configure a DS3/E3 port for service, see Figure 92 and Figure 93 on page 172 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.

2. From the expanded **CHASSIS** folder, select **Ports**.

3. On the **Ports** page, select the DS3 or E3 port being configured and click on **Properties**.

> **Note** The system displays all DS3/E3 ports in slots 2 and 3 if the system is equipped with DS3/E3 expansion modules in those slots.

> **Note** The system uses the following naming convention for DS3/E3 interfaces: T3:slot/port. For instance, T3:2/3 refers to the third DS3/E3 port in slot 2.

4. In the **Port Properties** window (see Figure 93), set **Admin Status** to **Enabled**.

You can use the port selector filters at the top of the **Ports** page to narrow the selection of ports according to port type and location. To display, for instance, only the DS3/E3 ports in slot 3, use the scroll-down buttons to select **Show DS3/E3 ports** and **Slot 3**. If you click on **Enable All Ports**, the system sets the **Admin Status** to **Enabled** for only the ports that are on display.

5. Set the **Line Rate** to **DS3** (default) or **E3**.

For DS3 ports, the line coding is set to B3ZS. For E3 ports, the line coding is set to HDB3. The system displays the correct line coding for the port after you click on **Apply** in Step 8.

6. Select the **Line Framing** for the DS3/E3 port.

Use the line framing setting if you wish to enable non-intrusive monitoring of DS3/E3 path-level defects and the collection of performance-monitoring data in both directions of transmission, that is, from the physical DS3/E3 port into the VC-3 (receive direction) and from the VC-3 into the physical port (transmit direction).

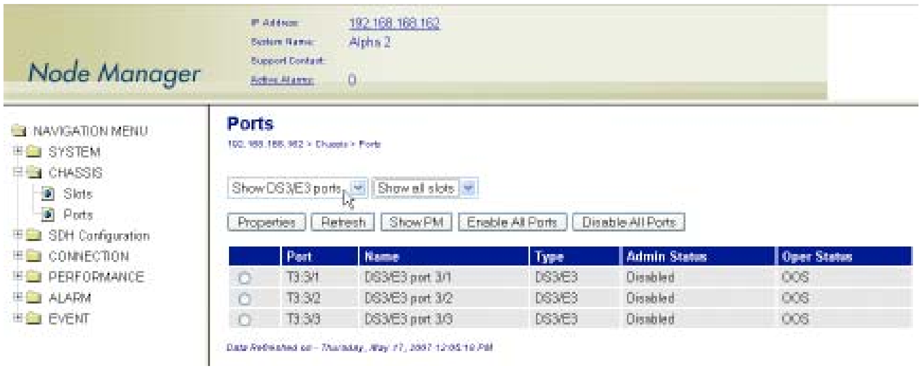
Make sure that the line framing setting corresponds to the actual frame structure of the DS3/E3 signal that is being monitored. For DS3 signals using C-bit parity framing, set the **Line Framing** to **C-bit Parity** to start the the collection of DS3 path PM data using both the P-bits and the CP-bits. For DS3 signals using M23 framing, set the **Line Framing** to **M23**; otherwise, setting the **Line Framing** to **C-bit Parity** results in the incorrect collection of PM data using the CP-bits.

> **Note** The system starts the collection of DS3/E3 path-monitoring data when the port is enabled and the framer is set to the correct signal frame structure.

7. Use the **Line Length (LBO meters)** scroll-down button to select the line-build out (LBO) settings for the DS3 port.

8. Click on **Apply** and then on **Close** to close the window.

On the **Ports** page, **Admin Status** for the selected DS3/E3 port should now read **Enabled**.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

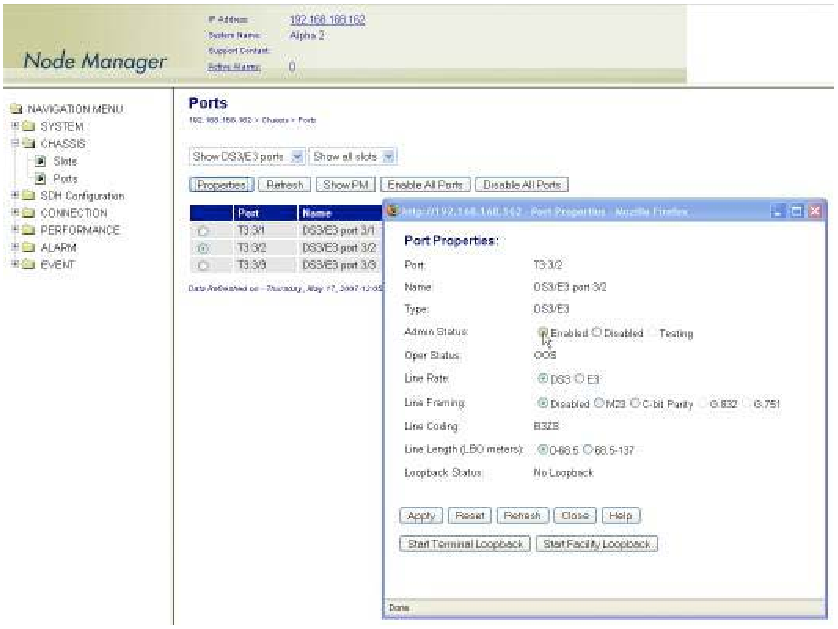
Ports

192.168.168.162 > Chassis > Ports

	Port	Name	Type	Admin Status	Oper Status
○	T3:3/1	DS3/E3 port 3/1	DS3/E3	Disabled	OOS
○	T3:3/2	DS3/E3 port 3/2	DS3/E3	Disabled	OOS
○	T3:3/3	DS3/E3 port 3/3	DS3/E3	Disabled	OOS

Data Refreshed on - Thursday, May 17, 2007 12:05:19 PM

Figure 92. Displaying DS3/E3 Ports



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

Ports

192.168.168.162 > Chassis > Ports

	Port	Name
○	T3:3/1	DS3/E3 port 3/1
●	T3:3/2	DS3/E3 port 3/2
○	T3:3/3	DS3/E3 port 3/3

Port Properties:

Port: T3:3/2
Name: DS3/E3 port 3/2
Type: DS3/E3
Admin Status: ● Enabled ○ Disabled ○ Testing
Oper Status: OOS
Line Rate: ● DS3 ○ E3
Line Framing: ● Disabled ○ M23 ○ C-bit Parity ○ G.832 ○ G.751
Line Coding: B3ZS
Line Length (LBO meters): ● 0-68.5 ○ 68.5-137
Loopback Status: No Loopback

Figure 93. Enabling a DS3/E3 Port

Note The operational status (**Oper Status**) for a DS3/E3 port is **IS** (in service) when the port **Admin Status** is **Enabled** and no alarms are present. Otherwise, the **Oper Status** for the port indicates **OOS** (out of service).

Disabling a Port from Service

To disable a DS3/E3 port from service, follow these steps:

1. In the **Port Properties** window, set **Admin Status** to **Disabled**.
2. Click on **Apply** and then on **Close** to close the window.

On the **Ports** page, **Admin Status** for the selected DS3/E3 port should now read **Disabled**.

Note When a DS3/E3 port is disabled, no port-related alarms are reported. PM data collection is also suspended. Furthermore, the system turns off the transmitter on the outgoing DS3/E3 signal.

Note The system inserts AIS into the VC-3 when a DS3/E3 port is disabled but remains connected to a TU-3 time slot.

DS3/E3 Connections

The following section describes the process of setting up and removing connections between DS3/E3 ports and SDH TU-3 time slots using asynchronous mapping into VC-3 termination points.

Creating a Port Connection

To connect a DS3/E3 port to a TU-3, see Figure 94 on page 175 and follow these steps:

1. Select the **CONNECTION** folder from the navigation menu.
2. From the expanded **CONNECTION** folder, select **Client Port Mappings**.

If no connections are present, the table on the **Client Port Mappings** page is empty.

3. On the **Client Port Mappings** page, use the **Create Mapping Options...** scroll-down button to select the **Create DS3/E3 Mapping** option.
4. In the **Create DS3/E3 Mapping** window, select the DS3/E3 port to be connected using the **DS3/E3 port** scroll-down button.

The system allows the creation of several DS3/E3 port connections at a time. To select more than one DS3/E3 port from the **DS3/E3 port** list, click on individual entries while pressing the Ctrl key. (The system highlights any entry that you select from the list. You can select any entry from the list, whether the E1 or T1 ports are contiguous or not.)

To select a range of consecutive entries from the list, select the first entry and then select the last entry while pressing the Shift key.

Use the Reset button to restore the window to the default selection.

Note The scroll-down list displays only the DS3/E3 ports that remain unconnected to TU-3s. The system displays and allows the connection of disabled DS3/E3 ports to TU-3s. A DS3/E3 port connected to a TU-3 sends AIS over the VC-3 TP when the port is disabled.

You may enable (or disable) a DS3/E3 port to activate (or deactivate) DS3/E3 service without deleting an existing connection. By connecting a DS3/E3 port to a TU-3 and leaving the port as disabled, you may test the connectivity and performance of the VC-3 path across the SDH network before allowing customer traffic from the port to pass across the STM-1 interface.

5. Select the TU-3 to which the port is to be connected using the **TU-3 Location** scroll-down button.

To select more than one TU-3 location from the **TU-3 Location** list, click on individual entries while pressing the Ctrl key. (The system highlights any entry that you select from the list. You can select any entry from the list, whether the TU-3 locations are contiguous or not.)

To select a range of consecutive entries from the list, select the first entry and then select thelast entry while pressing the Shift key.

Use the **Reset** button to restore the window to the default selection.

Note Make sure that the number of selected entries from the list matches the number of selected DS3/E3 ports in the **DS3/E3 port** list before proceeding; otherwise, the system rejects the creation of the connections.

Note The **TU-3 Location** for the TU-3 is indicated by the SDH indexing scheme (ST:1/1-U/K/L/M). The system displays the default **TU-3 Location** associated with the selected port. However, you can select any available TU-3 on the list.

The scroll-down list displays only the TU-3 time slots that remain unconnected.

6. If you wish to connect the DS3/E3 port to the TU-3 as a 2-way (bidirectional) connection, leave **Direction** as **2-way**.

However, for 1-way (unidirectional) connections, set **Direction** to **1-way**, and set the **Connection Point** button for **TU-3 Location** to indicate whether the TU-3 is the **Sink** or **Source** point for the connection.

For drop-and continue connections, set **Direction** to either **1-way drop-continue** or **2-way drop-continue**.

For multicast connections, set **Direction** to **1-way multicast**.

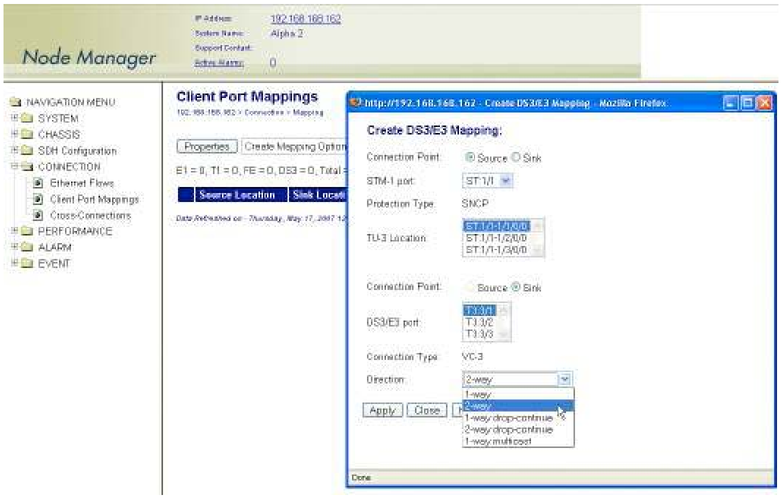
If you plan to drop DS3/E3 traffic from a single TU-3 into more than one DS3/E3 port in the same system slot, you must first start with the creation of a single 1-way multicast connection (and not with a regular 1-way connection) between the source TU-3 and the first of the DS3/E3 sink ports. Once the first multicast connection is present, you can add other multicast connection legs between the same TU-3 and other sink ports in the slot.

Note For Drop-and-continue and multicast connections, the system requires that the TU-3 is the source point of the connection.

7. Click on **Apply** to initiate the creation of the DS3/E3 connections.

CAUTION

The **Create DS3/E3 Mapping** window closes automatically after the system completes the creation of the DS3/E3 connections. If the number of connections is large, the system may take a few seconds to create the connections and close the window. Closing the window manually before.the process is complete may cause an error or partial creation of the new connections. Click on **Refresh** on the **Client Port Mappings** page to update the table with the new connections after the window closes.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

Client Port Mappings

192.168.168.162 > Connection > Mapping

E1 = 0, T1 = 0, FE = 0, DS3 = 0, Total =

Data Refreshed on - Thursday, May 17, 2007 12

http://192.168.168.162 - Create DS3/E3 Mapping - Mozilla Firefox

Create DS3/E3 Mapping:

Connection Point: ● Source ○ Sink

STM-1 port: ST 1/1

Protection Type: SNCP

TU-3 Location: ST 1/1-1/1/0/0 ST 1/1-1/2/0/0 ST 1/1-1/3/0/0

Connection Point: ○ Source ● Sink

DS3/E3 port: T3 3/1 T3 3/2 T3 3/3

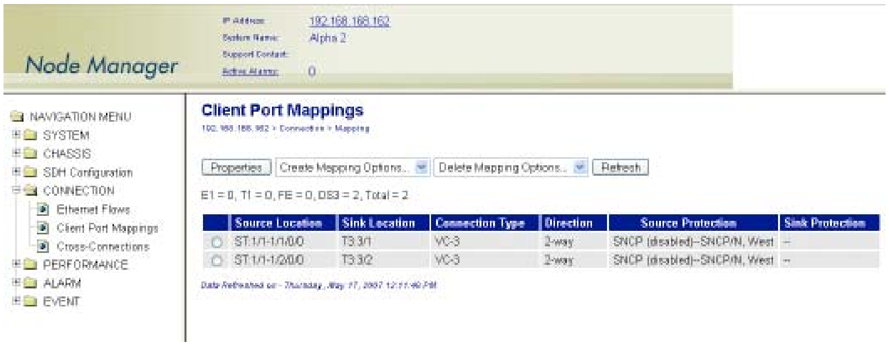
Connection Type: VC-3

Direction: 2-way

Figure 94. Connecting a DS3/E3 Port to a TU-3

The Client Port Mappings table now displays the newly made connections (see Figure 95).

Note The system enables the VC-3 TP into which the DS3/E3 signal is mapped only after the connection is made. Only at this point the TU-3 time slot that carries the VC-3 TP no longer sends the unequipped signal.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

Client Port Mappings

192.168.168.162 > Connection > Mapping

E1 = 0, T1 = 0, FE = 0, DS3 = 2, Total = 2

	Source Location	Sink Location	Connection Type	Direction	Source Protection	Sink Protection
○	ST 1/1-1/1/0/0	T3 3/1	VC-3	2-way	SNCP (disabled)--SNCP/N, West	--
○	ST 1/1-1/2/0/0	T3 3/2	VC-3	2-way	SNCP (disabled)--SNCP/N, West	--

Data Refreshed on - Thursday, May 17, 2007 12:11:40 PM

Figure 95. Displaying DS3/E3 Connections

Configuring the SNCP Protection Options for DS3/E3 Connections

If a DS3/E3 port is connected to an STM-1 port that supports SNCP protection, you can protect the connection end point using SNCP/I or SNCP/N.

To protect an existing DS3/E3 connection using SNCP, see Figure 96, and follow these steps:

1. On the **Client Port Mappings** page, select the table entry that contains the DS3/E3 connection that you wish to protect and click on **Properties**.
2. In the **Connection Properties** window, click on **SNCP Path Properties**.
3. In the **SNCP Path Properties** window, set **SNCP** to **Enabled**.

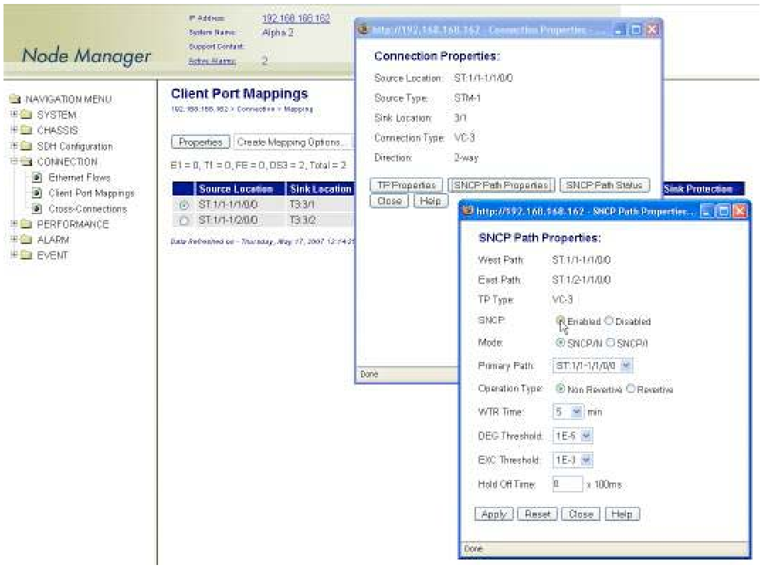
> **Note** SNCP can be enabled only if the DS3/E3 port is connected to STM-1 port 1 (west port).

At this time, you may change other SNCP path properties, including the **Mode** (SNCP/I or SNCP/N), **Operation Type** (non-revertive or revertive) and **Hold Off Time**. If the **Mode** is set to SNCP/N, you you may also change the **DEG Threshold** and **EXC Threshold**. (In SNCP/I mode, the system does not use the DEG and EXC thresholds to initiate the protection switch.)

At this time you may also change the **Primary Path** from STM-1 port 1 (west port) to STM-1 port 2 (east port).

> **Note** By default, the primary path in an SNCP connection is located on the west port. The primary and secondary paths are symmetrical. That is, both paths have the same TU-3 time slot index (U/K/L/M) on the east and west STM-1 ports.

4. Click on **Apply** and **Close** the **SNCP Path Properties** window.
5. **Close** the Connection Properties window.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 2

Client Port Mappings

192.168.168.162 > Connection > Mapping

E1 = 0, T1 = 0, FE = 0, DS3 = 2, Total = 2

	Source Location	Sink Location	Sink Protection
●	ST:1/1-1/1/0/0	T3:3/1	
○	ST:1/1-1/2/0/0	T3:3/2	

Data Refreshed on - Thursday, May 17, 2007 12:14:2

http://192.168.168.162 - Connection Properties - ...

Connection Properties:

Source Location: ST:1/1-1/1/0/0
Source Type: STM-1
Sink Location: 3/1
Connection Type: VC-3
Direction: 2-way

http://192.168.168.162 - SNCP Path Properties...

SNCP Path Properties:

West Path: ST:1/1-1/1/0/0
East Path: ST:1/2-1/1/0/0
TP Type: VC-3
SNCP: ● Enabled ○ Disabled
Mode: ● SNCP/N ○ SNCP/I
Primary Path: ST:1/1-1/1/0/0
Operation Type: ● Non Revertive ○ Revertive
WTR Time: 5 min
DEG Threshold: 1E-6
EXC Threshold: 1E-3
Hold Off Time: 0 x 100ms

Figure 96. Protecting DS3/E3 Connections Using SNCP

Configuring the J1 Trace

To configure the J1 trace message for the VC-3 TP that carries the DS3/E3 signal, see Figure 97 and follow these steps.

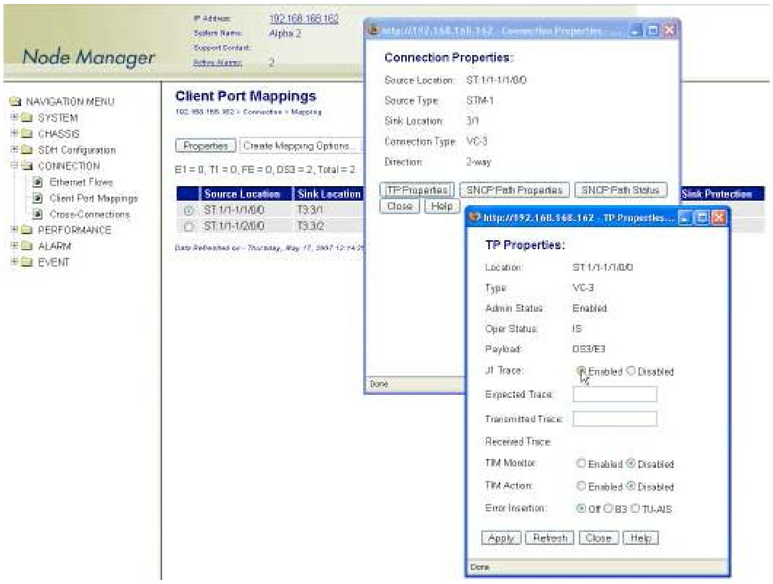
1. On the **Client Port Mappings** page, select the table entry for the required DS3/E3 connection and click on **Properties**.
2. In the **Connection Properties** window, click on **TP Properties**.
3. In the **TP Properties** window, set the **J1 Trace** to **Enabled**.
   - – Set **TIM Monitor** to **Enabled**, if you wish to detect trace identifier mismatch (TIM) defects for the VC-3 TP using the J1 trace.
   - – Set **TIM Action** to **Enabled**, if you wish to generate a consequent action (AIS downstream and LP-RDI upstream) upon detection of a TIM defect for the VC-3 TP using the J1 trace.
4. Type the **Expected Trace** and the **Transmitted Trace** using up to 15 ASCII characters for each field

Note The system inserts the transmitted trace into the outgoing J1 byte for the selected VC-3 TP.

5. Click on **Apply** and then on **Close** to close the **TP Properties** window.

Note The system does not allow enabling the J1 trace with the expected trace and transmitted trace fields empty. The system displays the **Received Trace** message if any is being received from the incoming J1 byte for the selected VC-3 TP.

6. Click on **Close** to close the Connection Properties window.



Client Port Mappings

192.168.168.162 > Connection > Mapping

E1 = 0, T1 = 0, FE = 0, DS3 = 2, Total = 2

	Source Location	Sink Location	Sink Protection
●	ST 1/1-1/1/0/0	T3 3/1	
○	ST 1/1-1/2/0/0	T3 3/2	

Data Refreshed on - Thursday, May 17, 2007 12:14:2

http://192.168.168.162 - Connection Properties

Connection Properties:

Source Location: ST 1/1-1/1/0/0

Source Type: STM-1

Sink Location: 3/1

Connection Type: VC-3

Direction: 2-way

http://192.168.168.162 - TP Properties...

TP Properties:

Location: ST 1/1-1/1/0/0

Type: VC-3

Admin Status: Enabled

Oper Status: IS

Payload: DS3/E3

J1 Trace: ● Enabled ○ Disabled

Expected Trace:

Transmitted Trace:

Received Trace:

TIM Monitor: ○ Enabled ● Disabled

TIM Action: ○ Enabled ● Disabled

Error Insertion: ● Off ○ B3 ○ TU-AIS

Figure 97. Configuring the J1 Trace

You can also configure the TP properties for all existing VC-3 TPs in the system by following these steps.

1. Select the **SDH Configuration** folder from the navigation menu.
2. From the expanded **SDH Configuration** folder, select **Termination Points**.
3. On the **Termination Points** page, select the table entry for the VC-3 TP that you wish to configure and click on **Properties**.
4. In the **TP Properties** window, you may know configure the J1 trace and the Error Insertion features for the selected VC-3 TP.
5. Click on **Close** to close the **TP Properties** window.

Removing a Port Connection

To remove an existing DS3/E3 port-to-TU-3 connection, follow these steps:

Step 1 Select a DS3/E3 port connection on the **Client Port Mappings** page.

Step 2 Click on **Delete** to remove the port connection.

At this point, the system removes the connection and it is no longer displayed in the table.

Note The system automatically disables the VC-3 TP after deletion of the connection to the TU-3 time slot. At this point, the system starts to send the unequipped signal over this TU-3. The time slot is now available for other connections.

DS3/E3 Alarms

The following section describes the process for monitoring alarms that may be present on DS3/E3 ports and the process of changing the default alarm settings.

Monitoring Port Alarms

Table 59 provides a list of the alarms that the system monitors at the DS3/E3 line level.

Table 59. DS3/E3 Line Alarms

Alarm	Description	Definition
DS3/E3 LOS	Loss of Signal	Incoming signal has no transitions for *n* consecutive pulse intervals

Note The system declares and displays an alarm condition if a defect persists for 2.5 ± 0.5 seconds. The alarm condition is cleared when the defect is terminated and remains absent for 10 ± 0.5 seconds.

The front panel of the 3-port DS3/E3 module provides an alarm status LED to indicate the presence of an active alarm condition of any severity level (Critical, Major, Minor, or Warning) on any of the three DS3/E3 ports on the module. The LED is lit according to the color codes in Table 60 on page 179.

Table 60. DS3/E3 Alarm Status LED

LED Color	Description
Green	No alarm is present on any port.
Amber	An alarm is present on one or more ports.
Off	All DS3/E3 ports are disabled.

To display DS3/E3 alarms, if present, see Figure 98 and follow these steps:

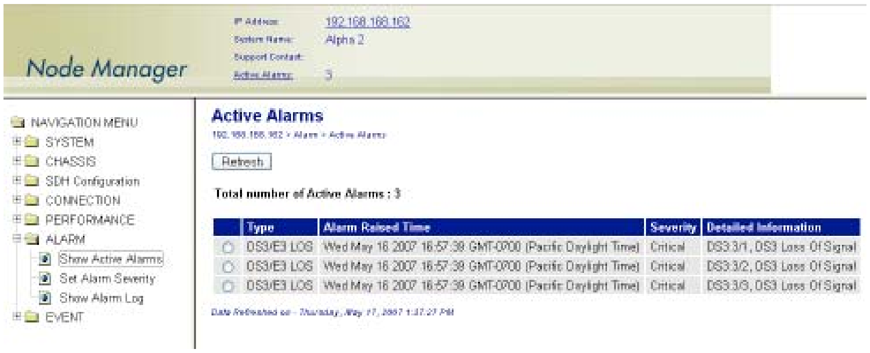
1. Select the ALARM folder from the navigation menu.
2. From the expanded ALARM folder, select Show Active Alarms.

At this point, the Active Alarms page displays all active alarms in the system, including DS3/E3 alarms, if present. The table contains a separate entry for each active alarm. Table 61describes the fields for each DS3/E3 alarm entry.

Table 61. Table Entries for Active DS3/E3 Alarms

Table Entry for Active Alarms	Field Value
Type	**LOS, Rx LOF, Tx LOF, Rx AIS, Tx AIS, Rx RAI, Tx RAI, Loopback**
Alarm Raised Time	Date and time
Severity	Critical, Major, Minor, or Warning
Detailed Information	Location of affected DS3/E3 port (T3:*slot/port* or E3:*slot/port*)

Note The system automatically updates the Active Alarms page every 60 seconds. Click on Refresh if you need to update the table with the most recent active alarm information. Individual table entries automatically clear whenever previously active alarms are no longer present.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 3

Active Alarms

192.168.168.162 > Alarm > Active Alarms

Total number of Active Alarms : 3

	Type	Alarm Raised Time	Severity	Detailed Information
○	DS3/E3 LOS	Wed May 16 2007 16:57:39 GMT-0700 (Pacific Daylight Time)	Critical	DS3 3/1, DS3 Loss Of Signal
○	DS3/E3 LOS	Wed May 16 2007 16:57:39 GMT-0700 (Pacific Daylight Time)	Critical	DS3 3/2, DS3 Loss Of Signal
○	DS3/E3 LOS	Wed May 16 2007 16:57:39 GMT-0700 (Pacific Daylight Time)	Critical	DS3 3/3, DS3 Loss Of Signal

Date Refreshed on - Thursday, May 17, 2007 1:37:27 PM

Figure 98. Displaying DS3/E3 Port Alarms

Changing Port Alarm Default Severities

Table 62 provides the default severities for DS3/E3 line alarms.

Table 62. DS3/E3 Line Alarm Default Severities

Monitored Entity	Near-end Alarm	Default Severity
DS3/E3 port	LOS	Critical

To change the default severity for supported DS3/E3 line alarms, follow these steps:

1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Set Alarm Severity.**

At this point, the **Alarm Severity** page displays a table with all supported system alarms.

3. Select the table entry containing the DS3/E3 port alarm **Type** (**DS3/E3 LOS**) and click on **Change.**
4. In the **Alarm Severity** window, set **Severity** to any desired level (**Critical, Major, Minor,** or **Warning**).
5. Click on **Apply** and then on **Close** to close the window.

On the **Alarm Severity** page, the **Severity** for the selected DS3/E3 port alarm **Type** should now reflect the change in the reported severity level.

Note The change applies to all DS3/E3 ports within the system.

Displaying the Alarm Log

To display historical alarms, including any DS3/E3 port alarms if present, follow these steps:

1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Show Alarm Log**.

At this point, the **Alarm Log** page displays a list of the 50 most recent alarm messages. The system keeps up to 500 entries in the alarm log.

Note The alarm log is a FIFO (first-in fist-out) log.

Click on **Last 50 Log Entries** or **Next 50 Log Entries** to move around and display the entire contents of the log. Click on **Clear Log** if you wish to delete permanently the current log entries.

DS3/E3 Performance Monitoring

The following section describes the process for displaying current and historical PM data for DS3/E3 ports.

Monitoring DS3/E3 Line Performance

Table 63 provides a list of the DS3/E3 line PM parameters (near-end) that the system monitors in accordance with G.826 and ANSI T1.231.

Table 63. DS3/E3 Line PM Parameters

Parameter	Description	Definition
LCV	Line Coding Violation	Count of BPV or EXZ over the accumulation period
LES	Line Errored Second	Count of seconds in which the LCV count is greater than or equal to 1 or in which a LOS defect occurs
LSES	Line Severely Errored Second	Count of seconds in which the LCV count is greater than or equal to 45 or in which a LOS defect occurs
LOSS	Loss of Signal Seconds	Count of seconds in which the LOS defect occurs

To display current line PM data for a DS3/E3 port, see Figure 99 on page 182 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the DS3/E3 port being configured and click on **Show PM**.

At this point, the **DS3/E3 Near-end PM** page shows the near-end line PM data for both the current 15-minute and 24-hour periods.

Note The PM data is not updated automatically as new events occur during the current 15-minute and 24-hour periods. Click on **Refresh** to update the tables with the most recent cumulative count for the current periods.

Continue with the steps that follow to display historical PM data.

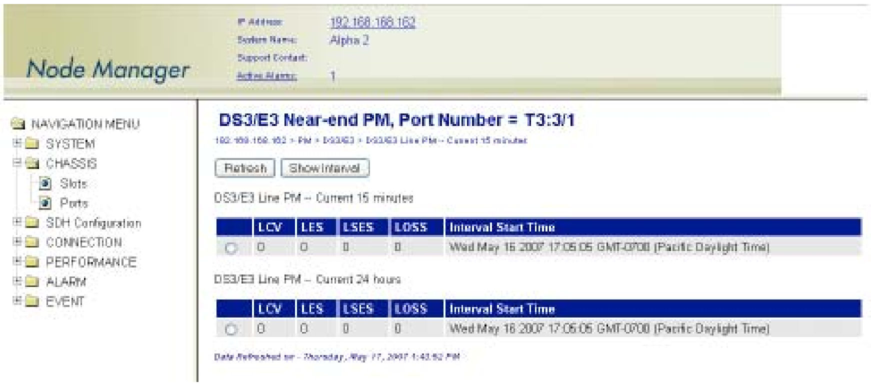
4. Click on **Show Interval**.

At this point, the **DS3/E3 Near-end PM** page shows the near-end line PM data for the following intervals:

- Current plus previous 95-by-15-minute intervals (24 hours total)
- Current plus previous day (2 days total)

Click on **Refresh** to update the tables with the most recent cumulative count for the current periods. This action updates only the first entry in the tables, which corresponds to the current measurement period.

Note The tables display **Invalid** under **PM data** when the data collected during a measurement period is considered invalid. The **Interval Start Time** also displays **n/a** (not available).



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 1

DS3/E3 Near-end PM, Port Number = T3:3/1

192.168.168.162 > PM > DS3/E3 > DS3/E3 Line PM -- Current 15 minutes

DS3/E3 Line PM -- Current 15 minutes

	LCV	LES	LSES	LOSS	Interval Start Time
○	0	0	0	0	Wed May 16 2007 17:05:05 GMT-0700 (Pacific Daylight Time)

DS3/E3 Line PM -- Current 24 hours

	LCV	LES	LSES	LOSS	Interval Start Time
○	0	0	0	0	Wed May 16 2007 17:05:05 GMT-0700 (Pacific Daylight Time)

Data Refreshed on - Thursday, May 17, 2007 1:43:52 PM

Figure 99. Displaying Current Line PM Data for DS3/E3 Ports

To display current and historical line PM data for all DS3/E3 ports in the system, see Figure 100 and follow these steps:

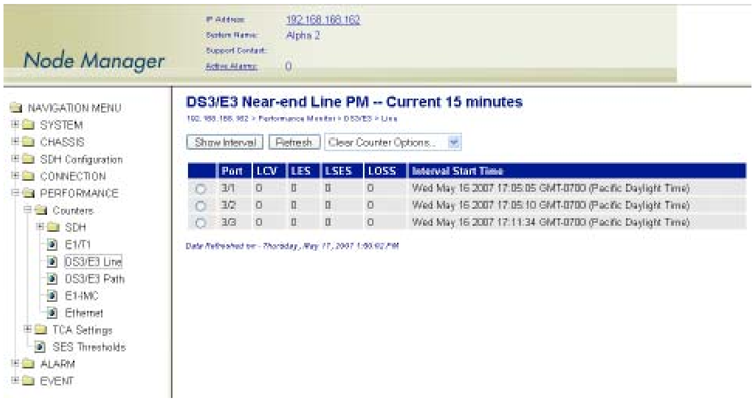
1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select **Counters**.
3. From the expanded **Counters** folder, select **DS3/E3 Line**.

At this point, the **DS3/E3 Near-end Line PM** page shows the near-end line PM data for the current 15-minute period only. The table displays PM data for only enabled DS3/E3 ports. (The table entries are empty if no DS3/E3 ports are enabled.)

Continue with the steps that follow to display historical line PM data for both 15-minute and 24-hour periods.

4. Select a DS3/E3 port and click on **Show Interval**.

> **Note** The preceding notes for the **DS3/E3 Near-end Line PM** page also apply to this procedure.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

DS3/E3 Near-end Line PM -- Current 15 minutes

192.168.168.162 > Performance Monitor > DS3/E3 > Line

	Port	LCV	LES	LSES	LOSS	Interval Start Time
○	3/1	0	0	0	0	Wed May 16 2007 17:05:05 GMT-0700 (Pacific Daylight Time)
○	3/2	0	0	0	0	Wed May 16 2007 17:05:10 GMT-0700 (Pacific Daylight Time)
○	3/3	0	0	0	0	Wed May 16 2007 17:11:34 GMT-0700 (Pacific Daylight Time)

Data Refreshed on - Thursday, May 17, 2007 1:50:02 PM

Figure 100. Displaying Current Line PM Data for All DS3/E3 Ports

To clear the current PM data for a DS3/E3 port, see Figure 100 on page 182 and follow this step:

1. On the **DS3/E3 Near-end Line PM** page, select a DS3/E3 port entry and use the **Clear Counter Options...** scroll-down button to select one of the available options for clearing the current 15-minute counter, 24-hour counter, or both.

Monitoring DS3/E3 Path Performance

Table 64 provides a list of the DS3/E3 path PM parameters (near-end) that the system monitors in accordance with G.826 and ANSI T1.231.

Table 64. DS3/E3 Path PM Parameters

Parameter	Description	Definition
PCV	P-bit Coding Violation	Count of P-bit parity errors over the accumulation period (M23 and C-bit parity)
PES	P-bit Errored Second	Count of seconds in which the PCV count is greater than or equal to 1 or in which an SEF or AIS defect occurs (M23 and C-bit parity)
PSES	P-bit Severely Errored Second	Count of seconds in which the PCV count is greater than or equal to 1 or in which an SEF or AIS defect occurs (M23 and C-bit parity)
SEF	Severely Errored Frame	Occurs upon detection of three or more F-bit errors in 16 consecutive F-bits.
UAS	Unavailable Second	Count of seconds in which the DS3/E3 path is unavailable. Period of unavailable time that begins at the onset of 10 consecutive PSES (M23 and C-bit parity) or CSES (C-bit parity only)
AISS	AIS Seconds	Count of seconds in which the AIS defect occurs.
CCV	C-bit Coding Violation	Count of CP-bit parity errors over the accumulation period (C-bit parity only).
CES	C-bit Errored Second	Count of seconds in which the CCV count is greater than or equal to 1 or in which an SEF or AIS defect occurs (C-bit parity only).
CSES	C-bit Severely Errored Second	Count of seconds in which the CCV count is greater than or equal to 45 or in which an SEF or AIS defect occurs (C-bit parity only).

To display current and historical path PM data for all DS3/E3 ports in the system, see Figure 101 on page 184 and follow these steps:

1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select **Counters**.
3. From the expanded **Counters** folder, select **DS3/E3 Path**.

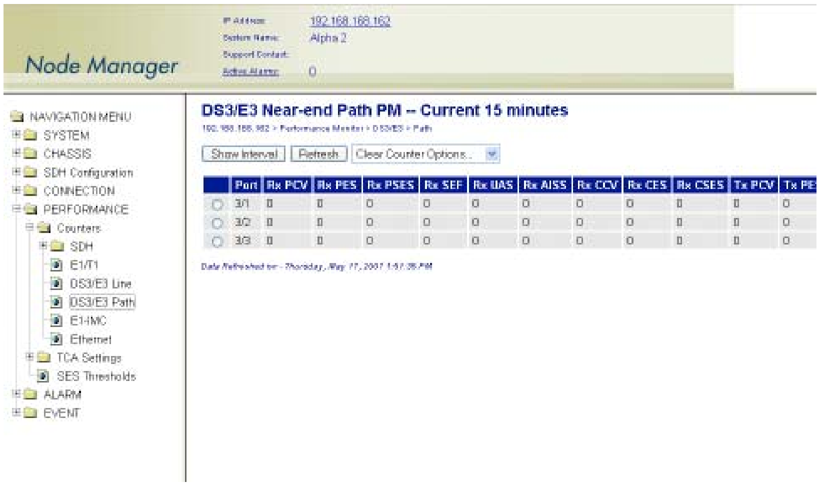
At this point, the **DS3/E3 Near-end Path PM** page shows the near-end path PM data for the current 15-minute period only. The table displays only PM data for enabled DS3/E3 ports. (The table entries are empty if no DS3/E3 ports are enabled.)

Note The system starts the collection of DS3/E3 path-monitoring data when the port is enabled and the framer is set to the correct signal frame structure. The system prefixes the DS3/E3 path PM parameters in Table 64 with "Rx" and "Tx" to indicate PM data in the receive and transmit directions, respectively.

Continue with the steps that follow to display historical path PM data for both 15-minute and 24-hour periods.

4. Select a DS3/E3 port and click on **Show Interval**.

Note The preceding notes for the **DS3/E3 Near-end Path PM** page also apply to this procedure.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

DS3/E3 Near-end Path PM -- Current 15 minutes

192.168.168.162 > Performance Monitor > DS3/E3 > Path

	Port	Rx PCV	Rx PES	Rx PSES	Rx SEF	Rx UAS	Rx AISS	Rx CCV	Rx CES	Rx CSES	Tx PCV	Tx PE
○	3/1	0	0	0	0	0	0	0	0	0	0	0
○	3/2	0	0	0	0	0	0	0	0	0	0	0
○	3/3	0	0	0	0	0	0	0	0	0	0	0

Date Refreshed on - Thursday, May 17, 2007 1:57:35 PM

Figure 101. Displaying Path PM Data for DS3/E3 Ports

Configuring DS3/E3 Port Threshold Crossing Alerts (TCA)

The system supports threshold registers for DS3/E3 line and path PM parameters. A TCA event is generated when a monitored event reaches or crosses the preset threshold value within a given measurement period (15 minutes or 24 hours).

TCA Settings for DS3/E3 Ports at the Line Level

To configure the system for reporting TCA events at the DS3/E3 line level, follow these steps:

Note By default, the reporting of TCA events for DS3/E3 ports at the line level is disabled.

1. Select the **EVENT** folder from the navigation menu.
2. From the expanded **EVENT** folder, select **Enable TCA Event**.
3. On the **TCA Event Disable /Enable** page, change **TCA Events** (**DS3/E3 Line**) to **On**.
4. Click on **Apply** to complete this task.

Note This is a global setting. Enabling the report of TCA events at the line level applies to all DS3/E3 ports on the system.

To configure the default TCA settings for DS3/E3 ports at the line level, follow these steps:

1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select the **TCA Settings** folder.
3. From the expanded **TCA Settings** folder, select the **DS3/E3 Line** folder.
4. From the expanded **DS3/E3 Line** folder, select **Default**.
5. On the **DS3/E3 Line Default TCA Settings** page, select the table entry and click on **Change**.
6. In the **DS3/E3 Line Default TCA Settings** window, change the default TCA settings for the DS3/E3 line LCV, LES, LSES and LOSS parameters (current and day periods) as required.

Note The system displays the factory default TCA settings when you first open this page. Later, the system displays any recent configuration changes.The preferred method of restoring the original settings is to re-enter the values manually.

7. Click on **Apply** and then on **Close** to close the **DS3/E3 Line Default TCA Settings** window.

Note The default values apply to all DS3/E3 ports on the system.

To assign custom TCA values for each individual DS3/E3 port on the system, continue with Step 8; otherwise, Step 7 completes this task.

8. From the expanded **DS3/E3 Line** folder, select **Custom**.

At this point, the **DS3/E3 Line TCA Settings** page displays the current line TCA settings for each DS3/E3 port on the system. The table entry indicates **Default** if the default TCA value is in use for a given parameter or **Custom** ***(value)*** if the system uses any custom value other than the default.

9. On the **DS3/E3 Line TCA Settings** page, select the DS3/E3 port that you wish to configure and click on **Change**.
10. In the **DS3/E3 Line TCA Settings** window, select **Custom** for the TCA settings that you wish to customize and change the setting to any value within the allowable range.

Note You may change the TCA settings for more than one parameter at a time.

11. Click on **Apply** and then on **Close** to close the **DS3/E3 Line TCA Settings** window.

At this point, the **DS3/E3 Line TCA Settings** page reflects any recent configuration changes.

If you wish to change a TCA setting back to its default setting, select **Default** instead of **Custom** in Step 10.

TCA Settings for DS3/E3 Ports at the Path Level

To configure the system for reporting TCA events at the DS3/E3 path level in the receive direction, follow these steps:

> **Note** By default, the reporting of TCA events for DS3/E3 ports at the path level is disabled.

1. Select the **EVENT** folder from the navigation menu.
2. From the expanded **EVENT** folder, select **Enable TCA Event**.
3. On the **TCA Event Disable /Enable** page, change **TCA Events** (**DS3/E3 Path Rx**) to **On**.
4. Click on **Apply** to complete this task.

> **Note** This is a global setting. Enabling the report of TCA events at the line level applies to all DS3/E3 ports on the system.

To configure the system for reporting TCA events at the DS3/E3 path level in the transmit direction, change **TCA Events** (**DS3/E3 Path Tx**) in Step 3 to **On**.

The steps to configure the default and custom TCA settings for DS3/E3 ports at the path level are the same as those for DS3/E3 ports at the line level but with the substitution of **DS3/E3 Line...** with **DS3/E3 Path...** The default and custom path TCA settings are the same for both receive and transmit directions.

DS3/E3 Testing

The following section provides the procedures for enabling and disabling loopback tests for DS3/E3 ports.

Configuring DS3/E3 Terminal Loopback

The OS-10 Series system supports terminal loopback for DS3/E3 ports. As shown in Figure 102, while the terminal loopback is active, the DS3/E3 signal is looped back toward the STM-1 interface just before transmission on the DS3/E3 physical interface. DS3/E3 AIS is also transmitted on the physical port.

Terminal loopback allows the testing of the performance and connectivity for a DS3/E3 service across the SDH network.

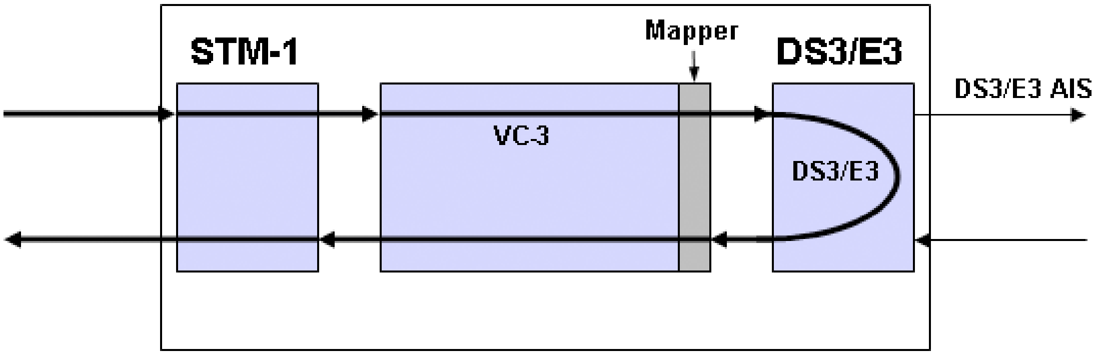


Figure 102. DS3/E3 Terminal Loopback

Configuring DS3/E3 Facility Loopback

The OS-10 system supports facility loopback for DS3/E3 ports, as shown in Figure 103. The loopback point occurs before mapping the DS3/E3 signal into a VC-3. If a connection is already present, the system inserts AIS into the VC-3 payload container (C-3) while the facility loopback is active. Facility loopback allows the testing of the performance and connectivity of the DS3/E3 cabling between the OS-10 and the end-user equipment.

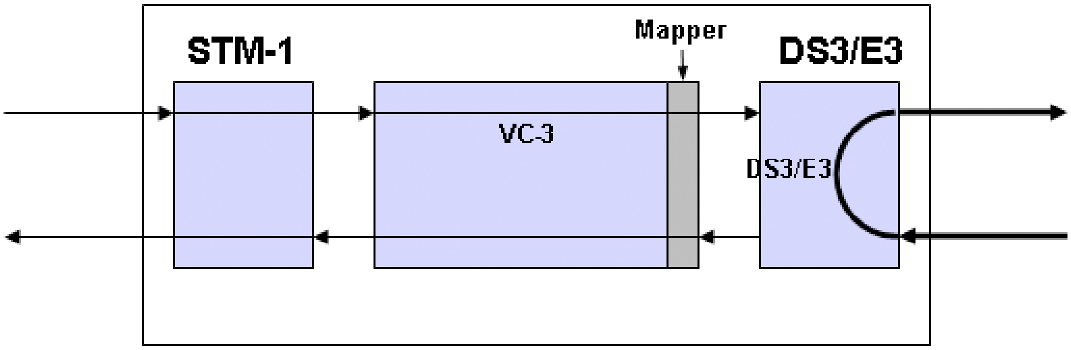


Figure 103. DS3/E3 Facility Loopback

To start a DS3/E3 terminal loopback (or facility loopback) test, see Figure 104 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the DS3/E3 port being tested and click on **Properties**.
4. In the **Port Properties** window, click on **Start Terminal Loopback** or **Start Facility Loopback**.

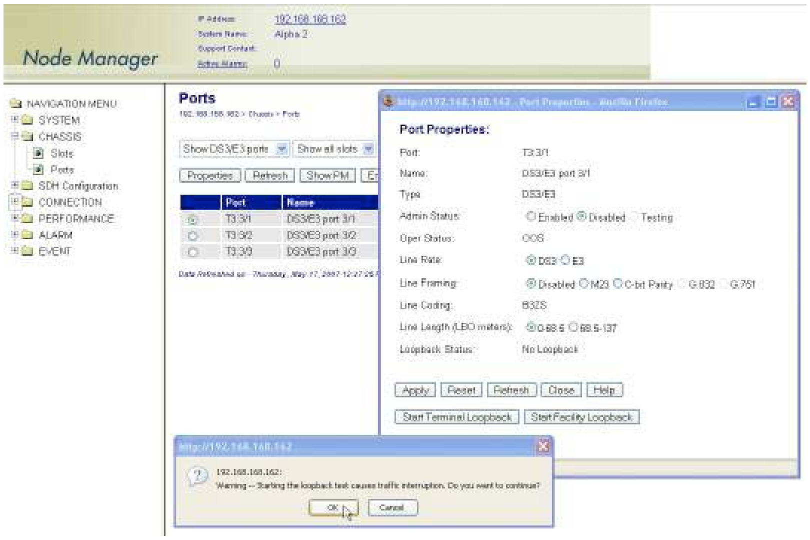
A warning window opens to alert you to the start of the loopback test. Click on **OK** to continue or **Cancel** to cancel the request.

WARNING

Starting a DS3/E3 terminal loopback causes traffic disruption if the DS3/E3 port is already connected to a TU-3.

Loopback Status on the **Port Properties** window changes to **Terminal Loopback Active** or **Facility Loopback Active. Admin Status** for the port changes to **Testing**.

5. Click on **Close** to close the Port Properties window.



IP Address: 192.168.168.162
System Name: Alpha 2
Support Contact:
Active Alarms: 0

Ports

192.168.168.162 > Chassis > Ports

	Port	Name
●	T3:3/1	DS3/E3 port 3/1
○	T3:3/2	DS3/E3 port 3/2
○	T3:3/3	DS3/E3 port 3/3

Data Refreshed on - Thursday, May 17, 2007 12:27:26

http://192.168.168.162 - Port Properties - Mozilla Firefox

Port Properties:

Port: T3:3/1
Name: DS3/E3 port 3/1
Type: DS3/E3
Admin Status: ○ Enabled ● Disabled ○ Testing
Oper Status: OOS
Line Rate: ● DS3 ○ E3
Line Framing: ● Disabled ○ M23 ○ C-bit Parity ○ G.832 ○ G.751
Line Coding: B3ZS
Line Length (LBO meters): ● 0-68.5 ○ 68.5-137
Loopback Status: No Loopback

http://192.168.168.162

192.168.168.162:
Warning -- Starting the loopback test causes traffic interruption. Do you want to continue?

Figure 104. Activating DS3/E3 Loopback

To stop a DS3/E3 loopback test, follow these steps:

1. In the **Port Properties** window, set **Admin Status** to **Enabled** or **Disabled**, if required.

2. Click on **Apply**.

At this point, **Loopback Status** changes to **No Loopback.** The system resumes any connection previously present between the DS3/E3 port and a TU-3 time slot.

3. Click on **Close** to close the the **Port Properties** window.

Chapter 6 Ethernet Interface

Chapter contents

Introduction

This chapter provides the procedures for provisioning, monitoring and testing of Ethernet client signal ports. Procedures for connecting Ethernet traffic to SDH are also provided.

General Information

The base OnSite OS1052 system has two (2) built-in Ethernet 10/100BASE-TX interfaces. Ethernet traffic is mapped into VCAT Groups (VCGs) using GFP encapsulation, as specified in ITU-T Recommendations G.7041/Y.1303 and G.707.

The Ethernet interfaces comply with the following standards:

- IEEE 802.3u (PHY)
- IEEE 802.3 (MAC)
- IEEE 802.3x (flow control)

The two Ethernet ports on the base system support frames in the following range: 64 to 9,600 bytes.

Figure 105 shows the location of Ethernet ports on the base OS1052 system.

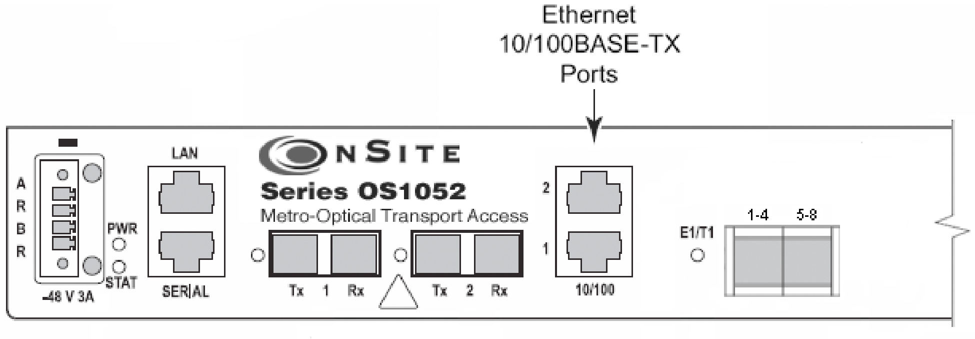


Figure 105. Ethernet Ports on the Base OS1052 System

The OS1052 also allows the insertion of an 8-port Ethernet expansion module for applications that require access to additional Ethernet ports (see chapter 13 for details on the HD-ENET module). With two modules, the OS1052 suports a total of up 18 Ethernet ports.

Likewise, the OS1063 supports insertion of two modules for a total of up to 16 Ethernet ports. Figure 106 shows an OS1063 system equipped with two 8-port Ethernet expansion modules.

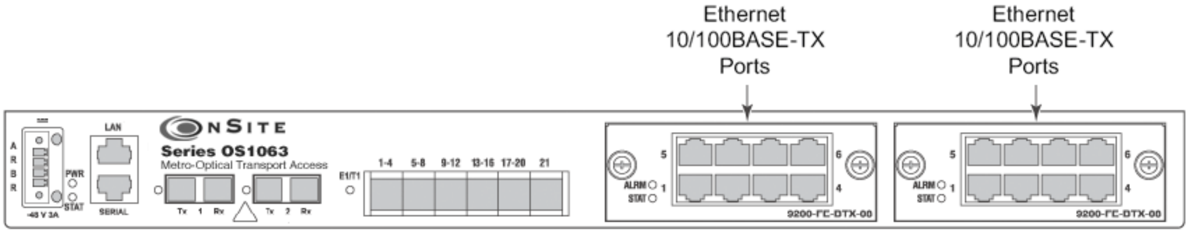


Figure 106. OS1063 with two Ethernet Expansion Modules

Table 65 provides the cabling specifications for the Ethernet ports.

Table 65. Ethernet Port Cabling Specifications

Cable	Specification
Connector	RJ-45
Type	Category 5
Reach	100m

Table 66 provides the pin assignment for the Ethernet RJ-45 connector.

Table 66. Ethernet Port Pin Assignment (RJ-45 Connector)

Signal Name	Description	RJ-45 Pin
RXN	Receive ring	6
RXP	Receive tip	3
TXN	Transmit ring	2
TXP	Transmit tip	1

Ethernet Provisioning

The following sections describe the procedures for enabling, disabling, and configuring the settings for Ethernet ports. The section concludes with the procedures for monitoring Ethernet port alarms and traffic statistics and setting up the Ethernet loopback test function.

Enabling a Port for Service

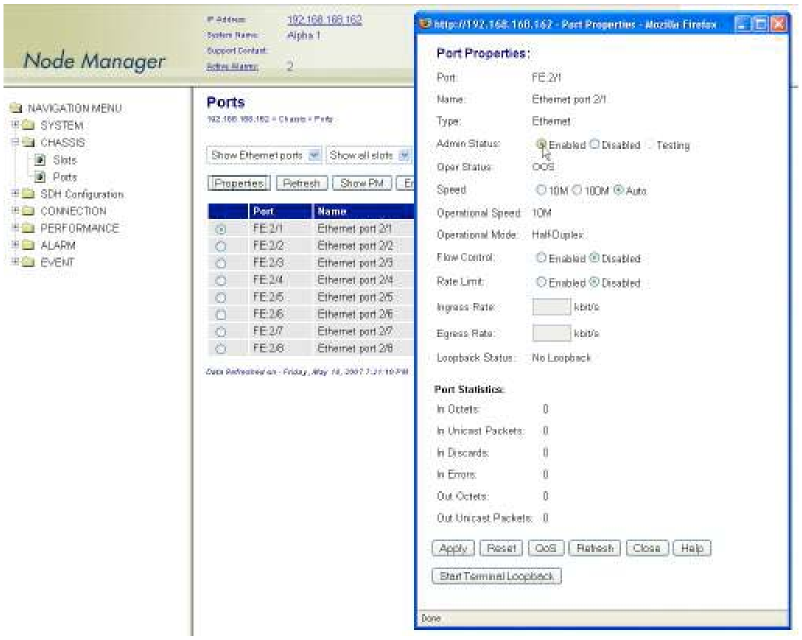
To configure an Ethernet port for service, see Figure 107 on page 192 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the Ethernet port being configured and click on **Properties**.

Note The system uses the following naming convention for Ethernet interfaces: FE:slot/port. The base OS1052 system contains two Ethernet ports in slot 1; that is, FE:1/1 and FE:1/2. (The OS1063 contains no Ethernet ports in slot 1). If the system has an 8-port Ethernet expansion module in slot 2, FE:2/5 would refer to Ethernet port 5 in slot 2.

4. In the **Port Properties** window, set the **Admin Status** to **Enabled**.
5. Click on **Apply** and then on **Close** to close the window.

On the **Ports** page, **Admin Status** for the selected Ethernet port should now read **Enabled**.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 2

Ports

192.168.168.162 > Chassis > Ports

	Port	Name
●	FE 2/1	Ethernet port 2/1
○	FE 2/2	Ethernet port 2/2
○	FE 2/3	Ethernet port 2/3
○	FE 2/4	Ethernet port 2/4
○	FE 2/5	Ethernet port 2/5
○	FE 2/6	Ethernet port 2/6
○	FE 2/7	Ethernet port 2/7
○	FE 2/8	Ethernet port 2/8

Data Refreshed on - Friday, May 18, 2007 7:21:10 PM

http://192.168.168.162 - Port Properties - Mozilla Firefox

Port Properties:

Port: FE 2/1
Name: Ethernet port 2/1
Type: Ethernet
Admin Status: ● Enabled ○ Disabled ○ Testing
Oper Status: OOS
Speed: ○ 10M ○ 100M ● Auto
Operational Speed: 10M
Operational Mode: Half Duplex
Flow Control: ○ Enabled ● Disabled
Rate Limit: ○ Enabled ● Disabled
Ingress Rate: kbit/s
Egress Rate: kbit/s
Loopback Status: No Loopback

Port Statistics:

In Octets: 0
In Unicast Packets: 0
In Discards: 0
In Errors: 0
Out Octets: 0
Out Unicast Packets: 0

Figure 107. Enabling an Ethernet port

Note The operational status (Oper Status) for an Ethernet port is IS (in service) when the port Admin Status is Enabled and no alarms are present (see §11.4). Otherwise, the Oper Status for the port indicates OOS (out of service).

Disabling a Port from Service

To disable an Ethernet port from service, see Figure 107 and follow these steps:

1. In the **Port Properties** window, set **Admin Status** to **Disabled**.
2. Click on **Apply** and then on **Close** to close the window.

On the **Ports** page, **Admin Status** for the selected Ethernet port should now read **Disabled**.

Note When an Ethernet port is disabled, no port-related alarms are reported (for example, Link Down). Data collection for port statistics is also suspended. Furthermore, the disabled port has the physical link down.

Configuring the Port Settings

This section describes the procedures for configuring the port settings of Ethernet ports, including: autonegotiation, flow control, rate control and QoS.

Autonegotiation

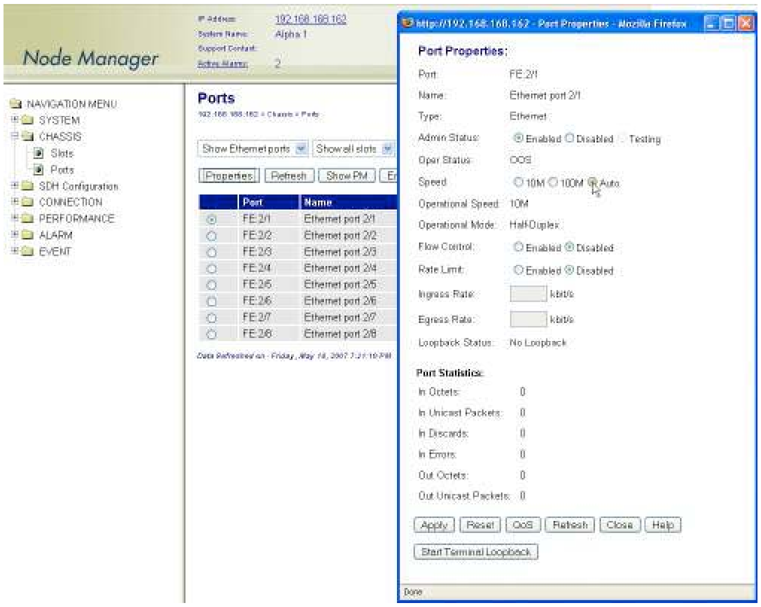
The system allows enabling or disabling autonegotiation for each Ethernet port. The default setting is enabled.

To enable Autonegotiation on an Ethernet port, see Figure 108 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the Ethernet port being configured and click on **Properties**.
4. In the **Port Properties** window, set **Speed** to **Auto**.

> **Note** By default, **Speed** is set to **Auto**.

5. Click on **Apply** and then on **Close** to close the window.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 2

Ports

192.168.168.162 > Chassis > Ports

	Port	Name
●	FE 2/1	Ethernet port 2/1
○	FE 2/2	Ethernet port 2/2
○	FE 2/3	Ethernet port 2/3
○	FE 2/4	Ethernet port 2/4
○	FE 2/5	Ethernet port 2/5
○	FE 2/6	Ethernet port 2/6
○	FE 2/7	Ethernet port 2/7
○	FE 2/8	Ethernet port 2/8

Data Refreshed on : Friday, May 18, 2007 7:21:10 PM

http://192.168.168.162 - Port Properties - Mozilla Firefox

Port Properties:

Port: FE 2/1
Name: Ethernet port 2/1
Type: Ethernet
Admin Status: ● Enabled ○ Disabled ○ Testing
Oper Status: OOS
Speed: ○ 10M ○ 100M ● Auto
Operational Speed: 10M
Operational Mode: HalfDuplex
Flow Control: ○ Enabled ● Disabled
Rate Limit: ○ Enabled ● Disabled
Ingress Rate: kbit/s
Egress Rate: kbit/s
Loopback Status: No Loopback

Port Statistics:

In Octets: 0
In Unicast Packets: 0
In Discards: 0
In Errors: 0
Out Octets: 0
Out Unicast Packets: 0

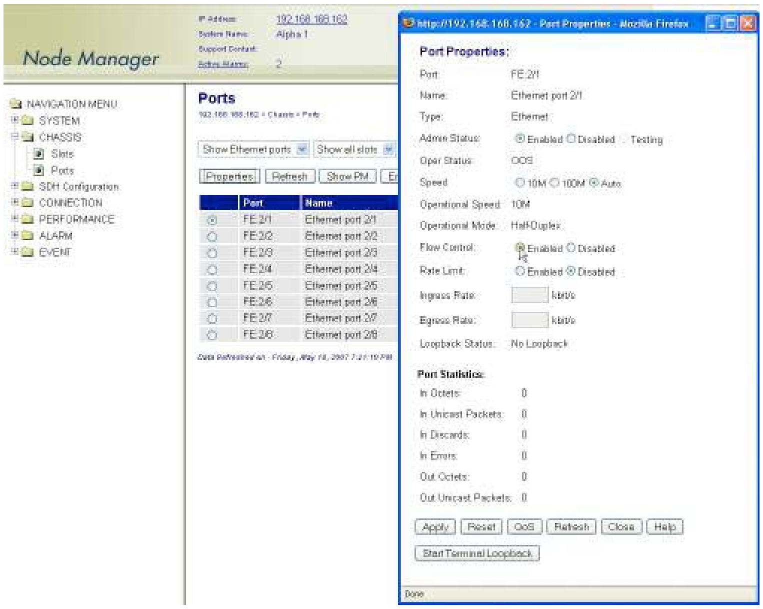
Figure 108. Configuring the Autonegotiation Option

Flow Control

The system allows enabling or disabling 802.3x flow control for each Ethernet port. The default setting is enabled.

To disable flow control on an Ethernet port, see Figure 109 on page 194 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the Ethernet port being configured and click on **Properties**.
4. In the **Port Properties** window, set **Flow Control** to **Disabled**.
5. Click on **Apply** and then on **Close** to close the window.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 2

Ports

192.168.168.162 > Chassis > Ports

	Port	Name
●	FE 2/1	Ethernet port 2/1
○	FE 2/2	Ethernet port 2/2
○	FE 2/3	Ethernet port 2/3
○	FE 2/4	Ethernet port 2/4
○	FE 2/5	Ethernet port 2/5
○	FE 2/6	Ethernet port 2/6
○	FE 2/7	Ethernet port 2/7
○	FE 2/8	Ethernet port 2/8

Data Refreshed on : Friday, May 18, 2007 7:21:10 PM

http://192.168.168.162 - Port Properties - Mozilla Firefox

Port Properties:

Port: FE 2/1
Name: Ethernet port 2/1
Type: Ethernet
Admin Status: ● Enabled ○ Disabled ○ Testing
Oper Status: OOS
Speed: ○ 10M ○ 100M ● Auto
Operational Speed: 10M
Operational Mode: Half-Duplex
Flow Control: ● Enabled ○ Disabled
Rate Limit: ○ Enabled ● Disabled
Ingress Rate: kbit/s
Egress Rate: kbit/s
Loopback Status: No Loopback

Port Statistics:

In Octets: 0
In Unicast Packets: 0
In Discards: 0
In Errors: 0
Out Octets: 0
Out Unicast Packets: 0

Figure 109. Configuring the Flow Control Option

Port Rate Control

The system allows enabling a rate control function for Ethernet ports on the high-density Ethernet (HDENET) expansion module. The rate control function works at the port level in both the ingress and egress directions of transmission.

> **Note** Ingress direction refers to traffic entering the system through the Ethernet client port. Egress direction refers to traffic leaving the system through the Ethernet client port.

To enable ratecontrol on an Ethernet port, see Figure 110 on page 195 and follow these steps:

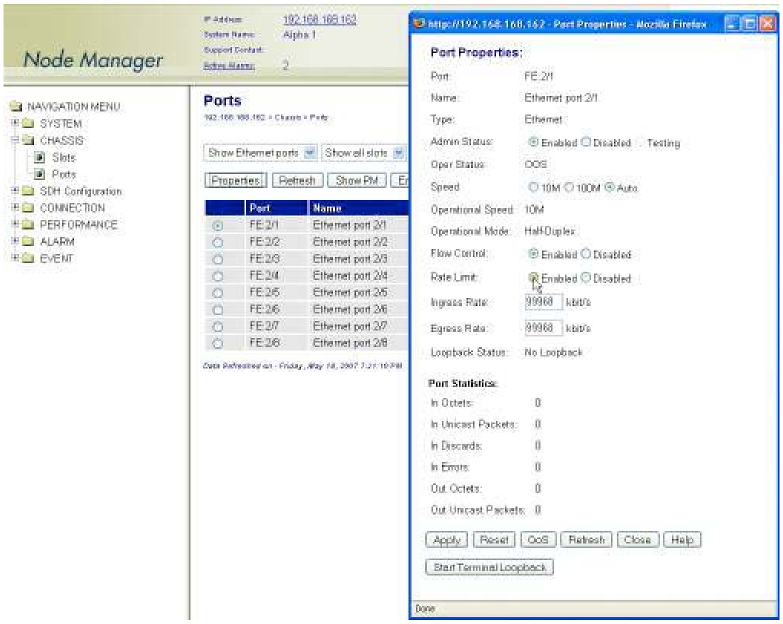
1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the Ethernet port being configured and click on **Properties**.

> **Note** Only Ethernet ports where the HD-ENET module is installed in slot 2 or 3 support configuration of the rate control parameters.

4. In the **Port Properties** window, set **Rate Limit** to **Enabled**.
5. Set the **Ingress Rate** and **Egress Rate** limit parameters for the port.

> **Note** You can set the rate control parameters in 64 kbit/s increments up to the full signal rate for the port. The system rounds up or down your entry to the nearest multiple of 64 kbit/s.

6. Click on **Apply** and then on **Close** to close the window.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 2

Ports

192.168.168.162 > Chassis > Ports

	Port	Name
●	FE 2/1	Ethernet port 2/1
○	FE 2/2	Ethernet port 2/2
○	FE 2/3	Ethernet port 2/3
○	FE 2/4	Ethernet port 2/4
○	FE 2/5	Ethernet port 2/5
○	FE 2/6	Ethernet port 2/6
○	FE 2/7	Ethernet port 2/7
○	FE 2/8	Ethernet port 2/8

Data Refreshed on - Friday, May 18, 2007 7:21:10 PM

http://192.168.168.162 - Port Properties - Mozilla Firefox

Port Properties:

Port: FE 2/1
Name: Ethernet port 2/1
Type: Ethernet
Admin Status: ● Enabled ○ Disabled Testing
Oper Status: OOS
Speed: ○ 10M ○ 100M ● Auto
Operational Speed: 10M
Operational Mode: HalfDuplex
Flow Control: ● Enabled ○ Disabled
Rate Limit: ● Enabled ○ Disabled
Ingress Rate: 99968 kbit/s
Egress Rate: 99968 kbit/s
Loopback Status: No Loopback

Port Statistics:

In Octets: 0
In Unicast Packets: 0
In Discards: 0
In Errors: 0
Out Octets: 0
Out Unicast Packets: 0

Figure 110. Configuring the Port Rate Control

Ethernet Port QoS

When Ethernet flows from multiple sources are aggregated into a single Ethernet port, it may be necessary to use the QoS functions of the port to ensure that individual packet flows are treated in accordance with user-defined priority markings for the application.

Each port on the high-density Ethernet (HD-ENET) expansion module (see chapter 13) has 4 transmission priority queues (0-3). Altogether, these queues can be configured in one of three packet scheduling modes: fair, strict priority (SP) and weighted fair queuing (WFQ).

Figure 111 shows an example of the use of QoS functions for the aggregation of Ethernet flows from multiple VCGs into a single Ethernet port. In this example, each egress flow from a VCG is manually assigned to a different transmit queue. (See §11.3 for details on Ethernet flows and connections.) The QoS settings for the port specify the manner in which the packet scheduler services the queues for transmission in the egress direction of the Ethernet port.

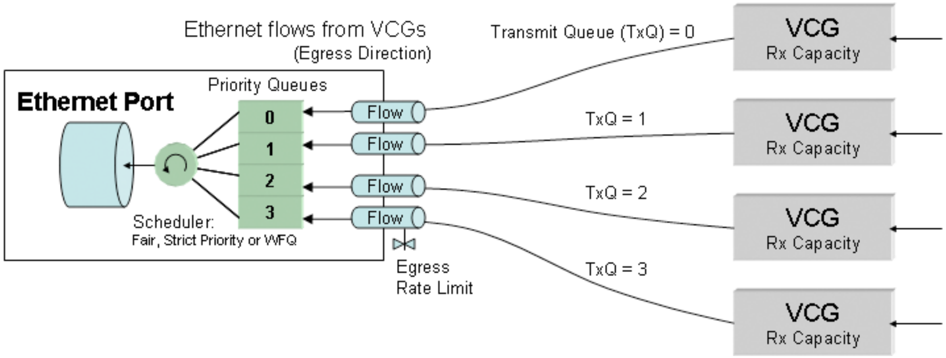


Figure 111. Application of Port QoS for the Aggregation of Ethernet Flows

To configure the QoS functions for an Ethernet port, see Figure 112 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select the Ethernet port being configured and click on **Properties**.

> **Note** Only Ethernet ports where the HD-ENET module is installed in slot 2 or 3 support configuration of the port QoS functions.

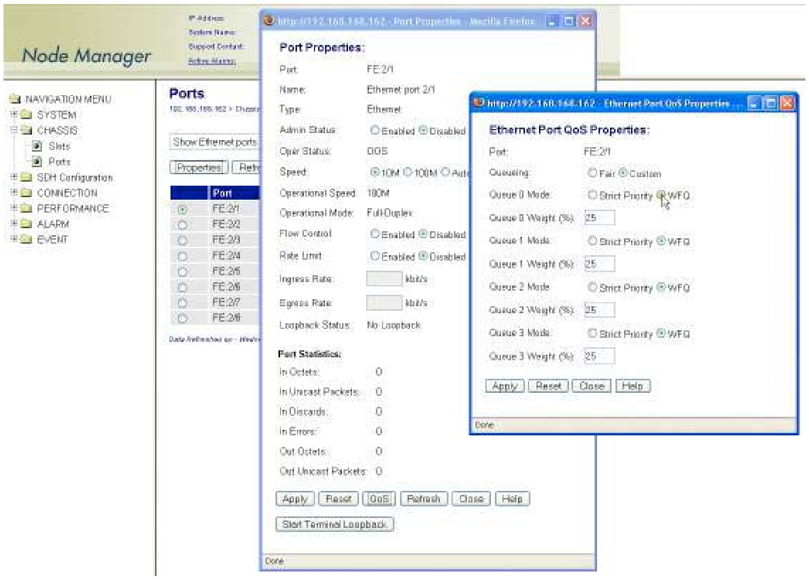
4. In the **Port Properties** window, click on **QoS.**
5. In the **Ethernet Port QoS Properties** window set **Queuing** to **Custom** if you wish to configure the packet scheduler for operation in Strict Priority or WFQ mode.
   - To configure the packet scheduler in **Strict Priority** mode, set **Queue 0 Mode** to **Strict Priority**. This change applies to all queues. (Strict Priority is the default setting for all queues.) Continue with Step 6 to complete this task.

In Strict Priority mode, the packet scheduler gives strict preference to packets in higher priority queues over packets in lower priority queues, regardless of the packet occupancy of individual queues. Among the four transmit queues, Queue 3 is the queue with the highest priority and Queue 0 is the queue with the lowest priority.

   - To configure the packet scheduler in **WFQ mode**, set **Queue 0 Mode** to **WFQ**. This change applies to all queues. Continue with Step 6 to complete this task.

In WFQ mode, the packet scheduler services the queues in accordance to a weight that you assign for each queue. The system requires that the sum of the weights for all four queues adds up to 100 percent.

6. Click on **Apply** and then on **Close** to close the **Ethernet Port QoS Properties** window.
7. Click on **Close** to close the **Port Properties** window.



● FE:2/1
○ FE:2/2
○ FE:2/3
○ FE:2/4
○ FE:2/5
○ FE:2/6
○ FE:2/7
○ FE:2/8

Port Properties:

Port:	FE:2/1
Name:	Ethernet port 2/1
Type:	Ethernet
Admin Status:	○ Enabled ● Disabled
Oper Status:	OOS
Speed:	● 10M ○ 100M ○ Auto
Operational Speed:	100M
Operational Mode:	FullDuplex
Flow Control:	○ Enabled ● Disabled
Rate Limit:	○ Enabled ● Disabled
Ingress Rate:	kbit/s
Egress Rate:	kbit/s
Loopback Status:	No Loopback

Port Statistics:

In Octets:	0
In Unicast Packets:	0
In Discards:	0
In Errors:	0
Out Octets:	0
Out Unicast Packets:	0

Ethernet Port QoS Properties:

Port:	FE:2/1
Queueing:	○ Fair ● Custom
Queue 0 Mode:	○ Strict Priority ● WFQ
Queue 0 Weight (%):	25
Queue 1 Mode:	○ Strict Priority ● WFQ
Queue 1 Weight (%):	25
Queue 2 Mode:	○ Strict Priority ● WFQ
Queue 2 Weight (%):	25
Queue 3 Mode:	○ Strict Priority ● WFQ
Queue 3 Weight (%):	25

Figure 112. Configuring the Ethernet Port QoS Function

Ethernet Connections

The following section describes the process of setting up and removing connections between Ethernet flows and VCAT groups (VCGs). The system supports three types of Ethernet flows: Port, VLAN, and SP-VLAN flows. Table 67 provides a description of these flows.

Table 67. Ethernet Flows in the OS-10 Series

Ethernet Flow Type	Consists of . . .
Port	All tagged and untagged frames from an Ethernet port
VLAN	A single customer-assigned VLAN ID or a range of consecutive VLAN IDs
SP-VLAN	A single service provider (SP) VLAN ID or a range of consecutive SP-VLAN IDs

Note VLAN and SP-VLAN flows can be created for only Ethernet ports on the high-density Ethernet expansion module (see chapter 13). The Ethernet ports on the OS1052 base system support only port flows.

Ethernet flows have two components: ingress and egress. For VLAN and SP-VLAN flows, the VLAN ID value is the same for both ingress and egress components. However, the system allows provisioning different rate control and priority settings (transmit queue and drop precedence) for each flow component.

You can set up a connection between an Ethernet flow and a VCG in one of three ways:

- Single flow from a port into a dedicated VCG
- Multiple flows from a port, each into a dedicated VCG
- Multiple flows from multiple ports, all into a shared VCG

Figure 113 shows the connection of a single flow from a port into a dedicated VCG. This type of connection is the most straightforward way of connecting Ethernet traffic for point-to-point private line applications. Here, the entire capacity of the VCG is allocated exclusively to the port, VLAN or SPVLAN flow.

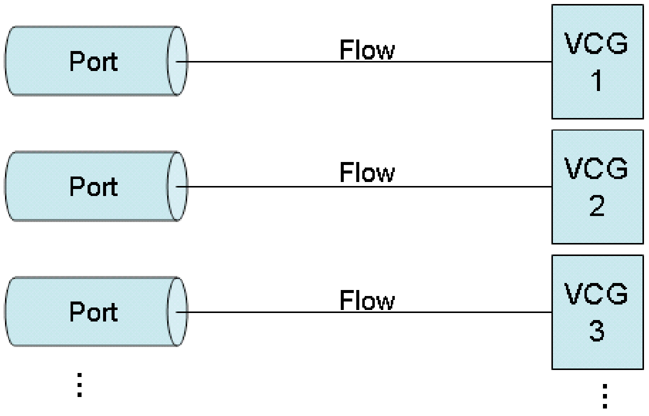


Figure 113. Single Flow from a Port into a Dedicated VCG

Figure 114 on page 198 shows the connection of multiple flows from a single port into individual VCG locations. This type of connection supports the aggregation of Ethernet traffic from multiple physical locations (each location served by one VCG) into one port.

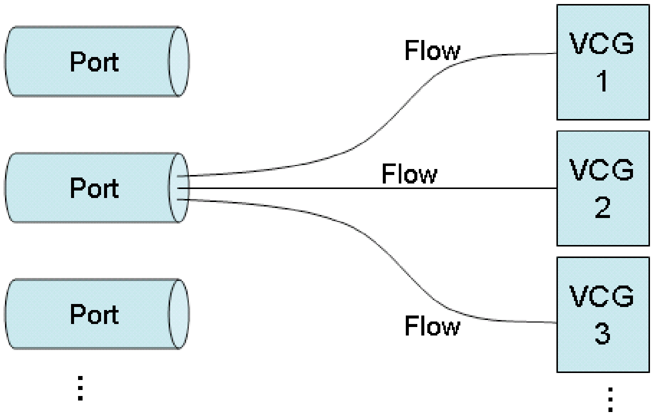


Figure 114. Multiple Flows from a Port into Dedicated VCGs

Figure 115 shows the connection of multiple flows from multiple ports into a single VCG. This type of connection provides maximum bandwidth efficiency when you need to transport Ethernet traffic from multiple sources to a common destination and the service requirements permit the use of priority-based packet scheduling to ensure fair access to the shared VCG capacity.

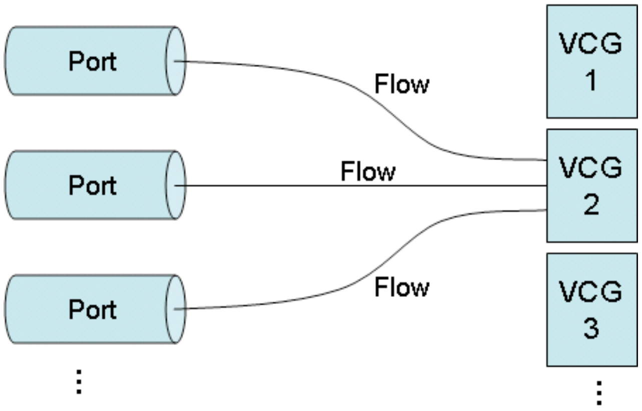


Figure 115. Multiple Flows from Multiple Ports into a Shared VCG

VLAN and SP-VLAN Connections

For VLAN flow connections, the system uses the customer-assigned VLAN tag (the C-Tag) to filter and connect Ethernet frames. You can configure the system to connect a single VLAN ID only or range of consecutive VLAN IDs. For example, in Figure 123, the system is configured to accept VLAN IDs 100 to 245. Only VLANs within the range are connected to the selected VCG.

Note The VLAN tag (or C-Tag) is defined by two values: the minimum and maximum VLAN IDs. You can use any value within the valid VLAN ID range of 0 to 4095. If both values are the same, the system selects only one VLAN ID instead of a range of consecutive VLAN IDs.

Note The system uses the EtherType for a C-Tag (0x8100) together with the VLAN ID to decide whether or not an Ethernet frame belongs to a VLAN flow or not. The system drops Ethernet frames that match the specified VLAN ID value for the VLAN flow but that have an EtherType other than 0x8100.

Figure 116 also shows a port flow connection. In this case, the VLAN ID filter is turned off and passes all incoming frames from the port for mapping into the VCG.

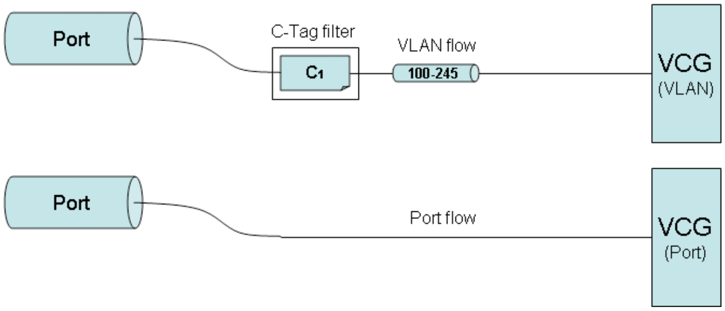


Figure 116. Dedicated Ethernet Port and VLAN Flow Connections

As shown in Figure 117, the system allows the connection of multiple VLAN flows into a single VCG. In this case, the VLAN ID (or range of IDs) must be unique for each flow that is mapped into the shared VCG capacity. The system enforces this rule as you create VLAN flow connections.

Note The VLAN ID values need to be different to ensure flow separation within the VCG and allow the far-end system that terminates the VCG to extract and connect the incoming flows into the correct Ethernet ports.

Note When you first connect a VLAN flow into a VCG that contains no other connections (the VCG is empty), the system classifies the VCG as a “VLAN”-type VCG. From this point, the system does not allow additional connections into the VCG other than VLAN. The system opens the VCG to other types of connections with the removal of the last VLAN connection from the VCG.

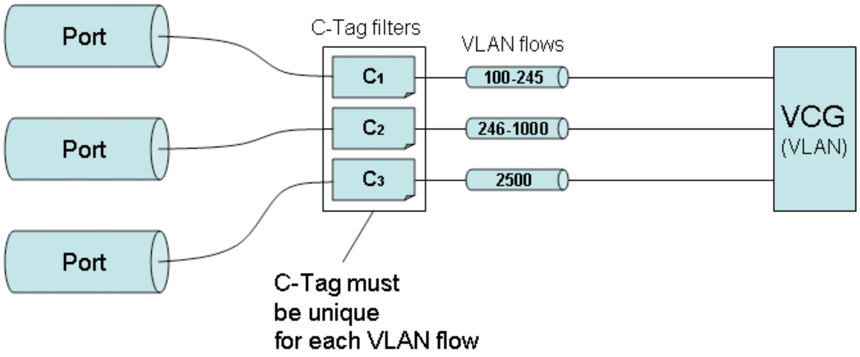


Figure 117. Shared Ethernet VLAN Flow Connections

For SP-VLAN flow connections, the system uses the service-provider VLAN tag (the S-Tag) to filter and connect Ethernet frames. You can configure the system to connect a single SP-VLAN ID only or range of consecutive SP-VLAN IDs. For example, in Figure 125, the system is configured to accept SP-VLAN IDs 100 to 245. Only SP-VLAN IDs within the range are connected to the selected VCG.

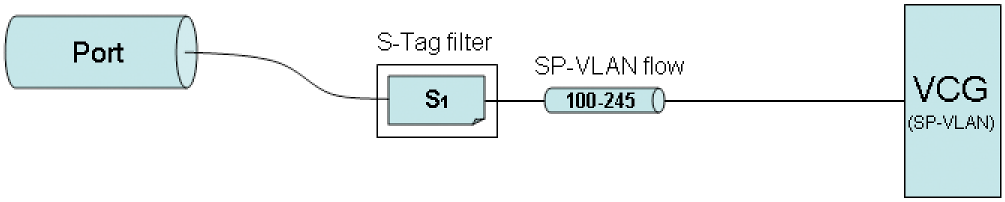


Figure 118. Dedicated Ethernet SP-VLAN Flow Connection

The SP-VLAN tag (or S-Tag) is defined by two values: the minimum and maximum SPVLAN IDs. You can use any value within the valid SP-VLAN ID range of 0 to 4095. If both values are the same, the filter selects only one SP-VLAN ID instead of a range of consecutive SPVLAN IDs.

The system uses the EtherType for an S-Tag (0x88a8) together with the SP-VLAN ID to decide whether or not an Ethernet frame belongs to an SP-VLAN flow or not. The system drops Ethernet frames that match the specified SP-VLAN ID value for the SP-VLAN flow but that have an EtherType other than 0x88a8.

As shown in Figure 119, the system allows the connection of multiple SP-VLAN flows into a single VCG. In this case, the SP-VLAN ID (or range of IDs) must be unique for each flow that is mapped into the shared VCG capacity. The system enforces this rule as you create SP-VLAN flow connections.

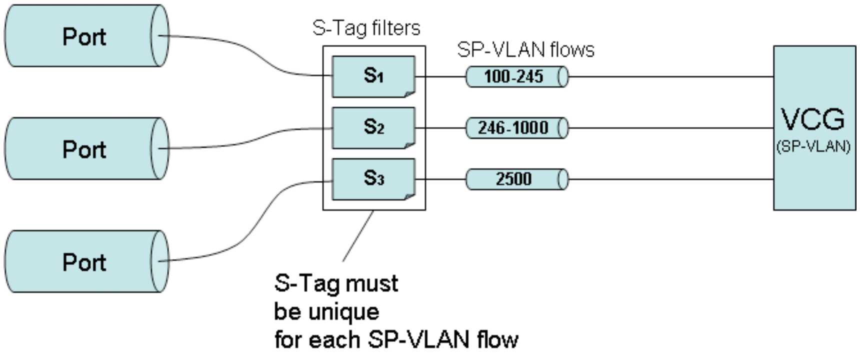


Figure 119. Shared Ethernet SP-VLAN Flow Connections

The SP-VLAN ID values need to be different to ensure flow separation within the VCG and allow the far-end system that terminates the VCG to extract and connect the incoming flows into the correct Ethernet ports.

When you first connect an SP-VLAN flow into a VCG that contains no other connections (the VCG is empty), the system classifies the VCG as an “SP-VLAN”-type VCG. From this point, the system does not allow additional connections into the VCG other than SP-VLAN. The system opens the VCG to other types of connection with the removal of the last SP-VLAN connection from the VCG.

C-Tag Connections

In addition to supporting the connection of native VLAN flows using the C-Tag information from an external source (such as a L2 switch or router), the system also lets you insert and remove a C-Tag that is fully under your control. This tagging operation is called “C-Tag Add/Strip.” When “C-Tag Add/Strip” is active, the OS-10 sytem performs two simultaneous functions for the selected Ethernet Port flow, as Table 68 indicates.

Note The system allows using the “C-Tag Add/Strip” tagging operation only for Ethernet Port flows. The operation is not available for VLAN and SP-VLAN flows.

Table 68. C-Tag Add/Strip Tagging Operation Functions

C-Tag Operation	Applies to. . .	Function
Add	Ingress flow direction	Insertion of C-Tag with VLAN ID specified by OS-10 user
Strip	Egress flow direction	Removal of C-Tag with VLAN ID specificed by OS-10 user

Note When you tag a Port flow with a C-Tag, the system classifies the connection as a C-Tag connection inside a VCG.

As shown in Figure 120, the system supports multiple C-Tag connections into a single VCG. In this case, the C-Tag must be unique for each Port flow that is mapped into the shared VCG capacity. The system enforces this rule as you create C-Tag connections.

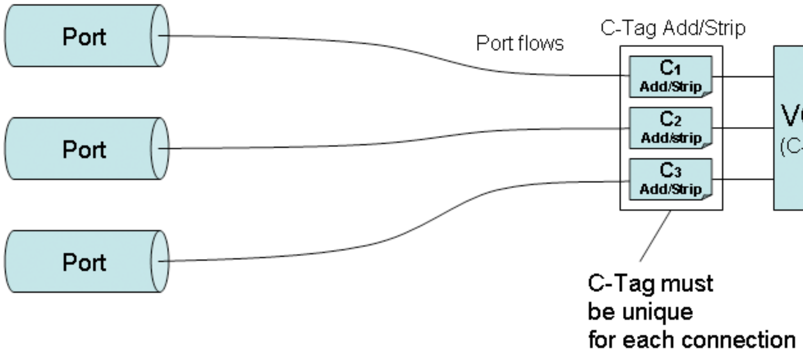


Figure 120. Shared Ethernet Port Flows Using C-Tag Connections

Note When you first make a C-Tag connection into a VCG that contains no other connections (the VCG is empty), the system classifies the VCG as a “C-Tag”-type VCG. From this point, the system does not allow additional connections into the VCG other than C-Tag. The system opens the VCG to other types of connection with the removal of the last C-Tag connection from the VCG.

S-Tag Connections

In addition to supporting the connection of native SP-VLAN flows using the S-Tag information from an external source (such as a L2 switch or router), the system also lets you insert and remove an S-Tag that is fully under your control. This tagging operation is called “S-Tag Add/Strip.” When “S-Tag Add/Strip” is active, the OS-10 performs two simultaneous functions for the selected Ethernet Port and VLAN flows, as Table 69 indicates.

Note The system allows using the “S-Tag Add/Strip” tagging operation only for Ethernet Port and VLAN flows. The operation is not available for SP-VLAN flows.

Table 69. S-Tag Add/Strip Tagging Operation Functions

S-Tag Operation	Applies to. . .	Function
Add	Ingress flow direction	Insertion of S-Tag with VLAN ID specified by OS-10 user
Strip	Egress flow direction	Removal of S-Tag with VLAN ID specificed by OS-10 user

When you tag a Port or VLAN flow with an S-Tag, the system classifies the connection as an S-Tag connection inside a VCG. For VLAN flows, the use of the S-Tag results in the insertion of a second VLAN tag for Q-in-Q tunneling.

As shown in Figure 121, you can use the S-Tag to combine multiple VLAN flows into a VCG, even when two or more flows have the VLAN ID number or range of IDs. The only requirement for the successful creation of a connection using the S-Tag is that the S-Tag number be unique within a VCG. The system enforces this rule as you create flow-based connections using the S-Tag.

Note The S-Tag values need to be different to ensure flow separation within the VCG and allow the far-end system that terminates the VCG to extract and connect the incoming flows into the correct Ethernet ports.

When you first make an S-Tag connection into a VCG that contains no other connections (the VCG is empty), the system classifies the VCG as an “S-Tag”-type VCG. From this point, the system does not allow additional connections into the VCG other than S-Tag. The system opens the VCG to other types of connection with the removal of the last S-Tag connection from the VCG.

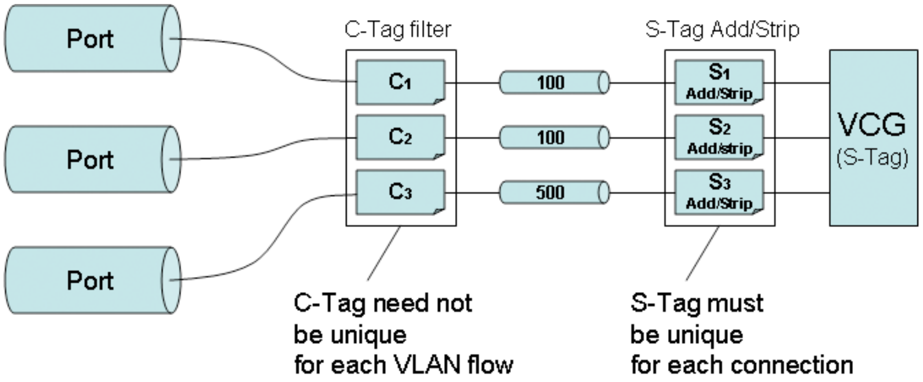


Figure 121. Shared Ethernet VLAN Flows Using S-Tag Connections

You can also use the S-Tag to combine Ethernet traffic from multiple ports into a single VCG (see Figure 122). In this case, the S-Tag is applied to all frames from the port, whether the frames are tagged or untagged. If the frames are untagged, the S-Tag results in the equivalent insertion of a VLAN tag with EtherType 0x88a8 and an ID number that is fully under your control.

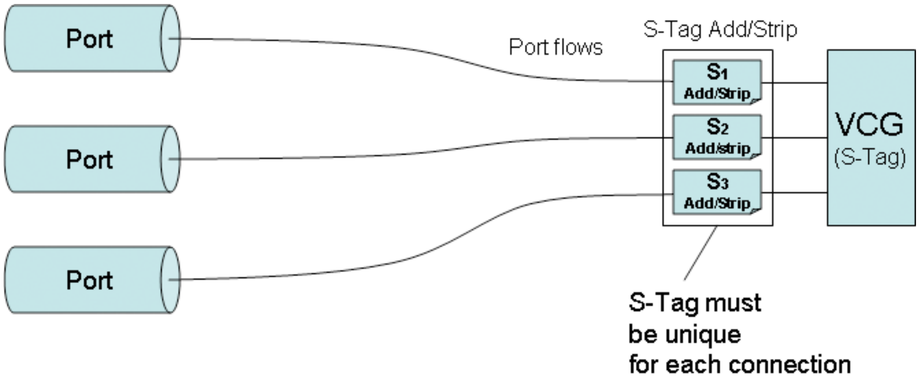


Figure 122. Shared Ethernet Port Flows Using S-Tag Connections

The S-Tag also provides the flexibility to combine a mix of Port and VLAN flows into a VCG, as shown in Figure 123.

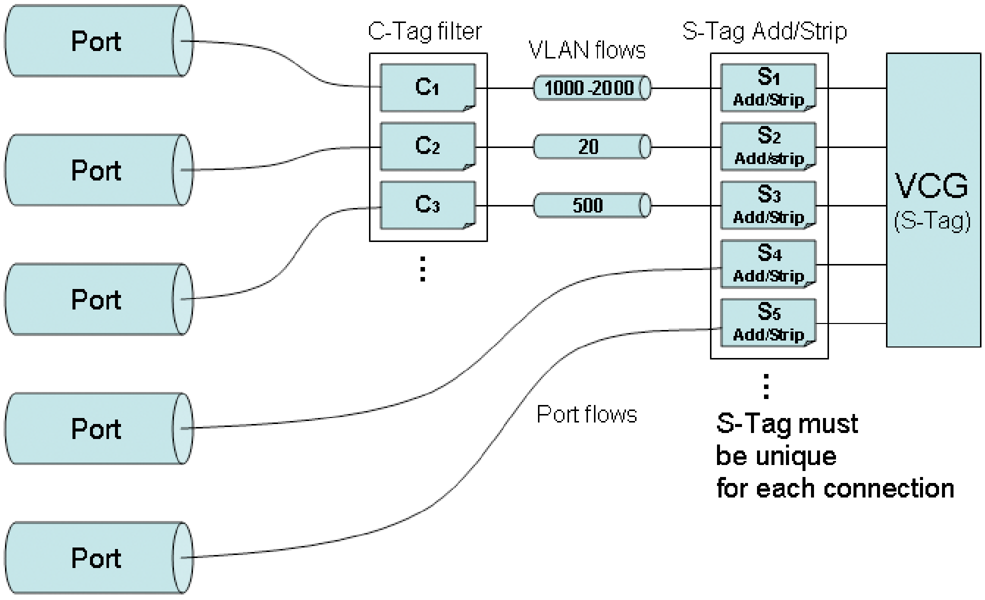


Figure 123. Shared Ethernet Port and VLAN Flows Using S-Tag Connections

Table 70 on page 204 provides a summary of the tagging operations that you can apply for different types of Ethernet flows. Note that for Port flows, you can apply both the C-Tag and S-Tag Add/Strip operations, but for VLAN flows, you can only apply the S-Tag Add/Strip operation. For SP-VLAN flows, none of the tagging operations are allowed. Furthermore, the table summarizes the connection types that result from the application of the tagging operations.

Table 70. Summary of Tagging Operations and Connections for Ethernet Flows

Ethernet Flow Type	Allowed Tagging Operations	Connection Type into VCG
Port	None	Port
	C-Tag (Add/Strip)	C-Tag
	S-Tag (Add/Strip)	S-Tag
VLAN	None	VLAN
	S-Tag (Add/Strip)	S-Tag
SP-VLAN	None	SP-VLAN

Creating a Connection

The following section contains the procedure for the connection of Ethernet flows into VCGs. The procedure starts with the steps to create a new Ethernet flow. Then, the procedure continues with the actual connection of the flow into one of the available VCGs.

To create an Ethernet flow, see Figure 124 on page 206 and follow these steps:

1. Select the **CONNECTION** folder from the navigation menu.
2. From the expanded **CONNECTION** folder, select **Ethernet Flows.**
3. On the **Ethernet Flows** page, click on **Add Flow.**
4. In the **Add Flow** window, select the ID number for the flow that you wish to create using the ID scroll-down button.

Note The system provides a list of the next available flow ID number for each Ethernet port in the system. For example, if there are no existing flows on port FE:3/8, the next available flow ID number for that port would be FE:3/8-1 (that is, the first flow). If, however, the port already has two flows configured, the system displays FE:3/8-3 as the next available flow ID number.

5. Type the **Name** for the flow if you wish to identify the new flow with an alphanumeric string. Otherwise, leave the field empty and continue with Step 6.
6. Select the **Type** of flow that you wish to create: **Port**, **VLAN** or **SP-VLAN**.
   - Select **Port** if you wish to connect the entire port into a VCG.
   - Select **VLAN** if you wish to connect a specified VLAN ID or range of VLAN IDs from the port into a VCG.
   - Select **SP-VLAN** if you wish to connect a specified service provider (SP) VLAN ID or range of SP-VLAN IDs from the port into a VCG.

Note VLAN and SP-VLAN flows can be created for only Ethernet ports on the high-density Ethernet expansion module.

7. If you select VLAN or SP-VLAN as the flow type in Step 6, type the **Min VLAN ID** and **Max VLAN ID** fields. Otherwise, go to Step 8.

> **Note** The valid range of VLAN ID values is 0 to 4095. If you wish to select only one VLAN ID from the port, use the same value for Min VLAN ID and Max VLAN ID. If you wish to define the flow as a range of consecutive VLAN IDs from the port, use different values for Max VLAN ID and Min VLAN ID. You can use any VLAN ID values within the valid range of 0 to 4095. For SP-VLAN flows, the system uses the S-Tag to filter and connect Ethernet packets with the specified VLAN ID values and with EtherType value of 0x88a8.

The system filters incoming Ethernet traffic according to the specified VLAN settings. All untagged Ethernet frames are dropped, and only VLAN-tagged frames within the specified Min VLAN ID and Max VLAN ID range are allowed to pass through.

8. If you wish to limit the rate at which the flow is connected to a VCG, set **Rate Control** to **Enabled** and type the **Sustained Rate** and **Peak Rate** parameters for both the ingress and egress directions of transmission. You can set the rate control parameters in 64 kbit/s increments up to the full signal rate for the port. The system rounds up or down your entry to the nearest multiple of 64 kbit/s.

9. If you plan to connect this flow to a VCG that contains other flows (that is, a shared VCG), select the **Transmit Queue** and **Drop Precedence** for both the ingress and egress directions of transmission.

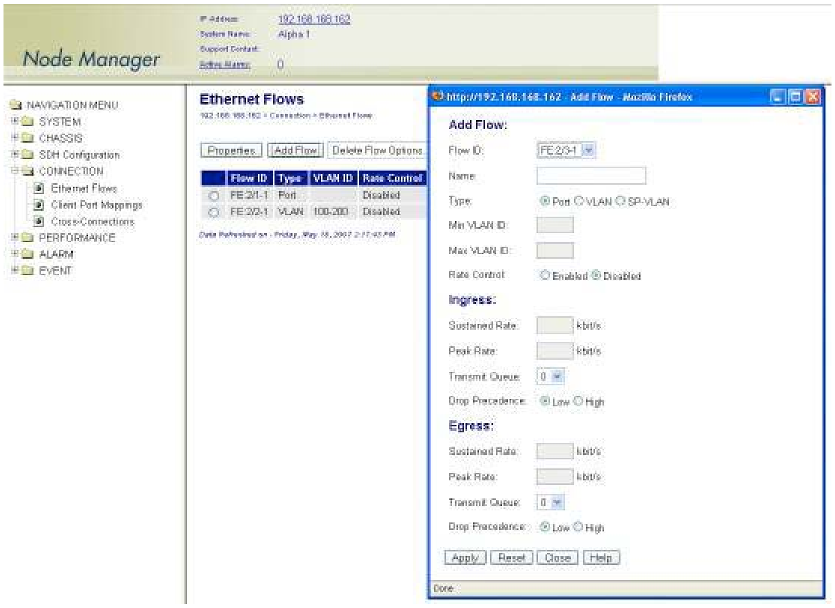
For the **Ingress** component of the flow (that is, from the Ethernet client port towards the VCG), the **Transmit Queue** indicates the queue number of the VCG into which the system connects the flow. The system uses the QoS settings of the VCG to schedule packet transmission from the queues towards the VCG capacity.

For the **Egress** component of the flow (that is, from the VCG towards the Ethernet client port), the **Transmit Queue** indicates the queue number of the Ethernet port into which the system connects the flow. The system uses the QoS settings of the Ethernet port to schedule packet transmission from the queues towards the Ethernet port capacity. (See §11.2.3.4 for details on configuring the QoS settings of an Ethernet port.)

For each flow component, the **Drop Precedence** indicates whether the frames belonging to the flow are of high-drop or low-drop classification. The system uses WRED (weighted random early discard) to discard frames in a gradual, graceful, and randomly selected manner before internal congestion occurs. The system drops frames with **High** drop precedence with higher probability than frames with Low drop precedence.

10. Click on **Apply** and then on **Close** to close the window.

At this point, the flow is configured for service and is ready for connection to a selected VCG.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Ethernet Flows

192.168.168.162 > Connection > Ethernet Flows

	Flow ID	Type	VLAN ID	Rate Control
○	FE:2/1-1	Port		Disabled
○	FE:2/2-1	VLAN	100-200	Disabled

Data Refreshed on - Friday, May 18, 2007 2:17:45 PM

Add Flow:

Flow ID: FE:2/3-1

Name:

Type: ● Port ○ VLAN ○ SP-VLAN

Min VLAN ID:

Max VLAN ID:

Rate Control: ○ Enabled ● Disabled

Ingress:

Sustained Rate: kbit/s

Peak Rate: kbit/s

Transmit Queue: 0

Drop Precedence: ● Low ○ High

Egress:

Sustained Rate: kbit/s

Peak Rate: kbit/s

Transmit Queue: 0

Drop Precedence: ● Low ○ High

Figure 124. Creating an Ethernet Flow

To connect an Ethernet flow to a VCG, see Figure 125 on page 207 and follow these steps:

1. Select the **CONNECTION** folder from the navigation menu.
2. From the expanded **CONNECTION** folder, select **Client Port Mappings**.
3. On the **Client Port Mappings** page, use the **Create Mapping Options...** scroll-down button to select the **Create Ethernet Mapping** option.

> **Note** If no Ethernet flows are available for new connections, the system responds with a warning message. You can proceed only if there are any existing flows that remain unconnected within the system.

4. In the **Create Ethernet Mapping** window, select the VCAT group to which you wish to connect the Ethernet flow using the **VCG ID** scroll-down button.

> **Note** If no flow matches the selected VCG ID, the system responds with a warning message. Change the VCG ID selection until the Flow ID presents a list of flows that contains the flow that you wish to connect to the VCG.

5. Select the Ethernet flow that you wish to connect, using the **Flow ID** scroll-down button.

> **Note** The flow Type indicates whether the selected flow is a port, VLAN or SP-VLAN flow and the VLAN ID range for VLAN and SP-VLAN flows.

6. If you wish to connect the flow to the VCG using an S-Tag, set **Tagging Operation** to **S-Tag (Add/Strip)** and type the **Tag ID** for the **S-VID** (0 to 4095). On the other hand, if you wish to connect the flow to the VCG using a C-Tag, set **Tagging Operation** to **C-Tag (Add/Strip)** and type the **Tag ID** for the **C-VID** (0 to 4095). Otherwise, for non-tagged connections, leave **Tagging Operation** as **None**.

> **Note** The S-Tag (or C-Tag) ID value must be unique within the VCG if the VCG already supports other flow connections that use the S-Tag (or C-Tag).

7. If you wish to connect the flow to the VCG as a 2-way (bidirectional) connection, leave **Direction** as **2-way**. However, for 1-way (unidirectional) connections, set **Direction** to **1-way**, and set the **Connection Point** button for **VCAT Group (VCG)** to indicate whether the VCG is the **Sink** or **Source** point for the connection.

For drop-and continue connections, set **Direction** to either **1-way drop-continue** or **2-way drop-continue**.

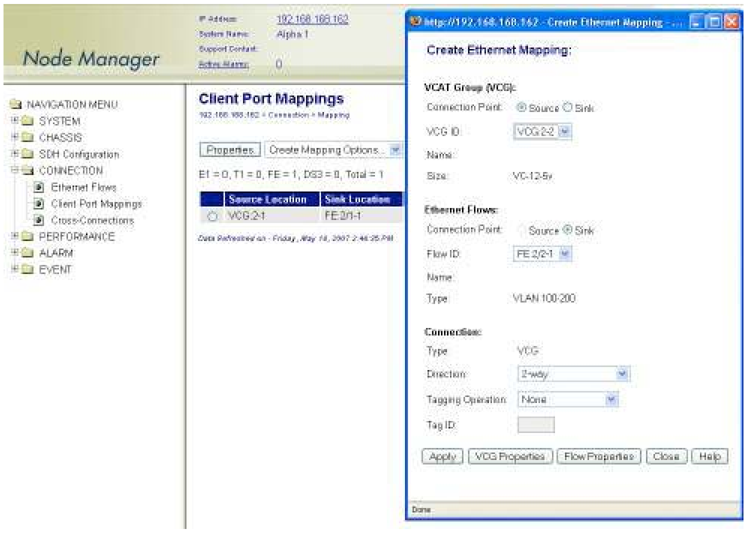
For multicast connections, set **Direction** to **1-way multicast**.

If you plan to drop Ethernet traffic from a single VCG into more than one Ethernet port in the same expansion slot, you must first start with the creation of a single 1-way multicast connection (and not with a regular 1-way connection) between the source VCG and the first of the Ethernet sink ports. Once the first multicast connection is present, you can add other multicast connection legs between the same VCG and other sink ports in the slot.

For Drop-and-continue and multicast connections, the system requires that the VCG is the source point of the connection.

8. Click on **Apply** and then on **Close** to close the widow.

At this point, the **Client Port Mappings** page displays the new connection between the selected flow and VCG. For each flow connection, the **Connection Type** indicates whether a flow connects to the VCG at the Port, VLAN, SP-VLAN, C-Tag, or S-Tag level. The Ethernet ports on the base OS1052 system support the use of the C-Tag and S-Tag Add/Strip operations.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Client Port Mappings
192.168.168.162 > Connection > Mapping

E1 = 0, T1 = 0, FE = 1, DS3 = 0, Total = 1

	Source Location	Sink Location
○	VCG 2-1	FE 2/1-1

Data Refreshed on - Friday, May 18, 2007 2:46:25 PM

http://192.168.168.162 - Create Ethernet Mapping - ...

Create Ethernet Mapping:

VCAT Group (VCG):
Connection Point: ● Source ○ Sink
VCG ID: VCG 2-2
Name:
Size: VC-12-5v

Ethernet Flows:
Connection Point: ○ Source ● Sink
Flow ID: FE 2/2-1
Name:
Type: VLAN 100-200

Connection:
Type: VCG
Direction: 2-way
Tagging Operation: None
Tag ID:

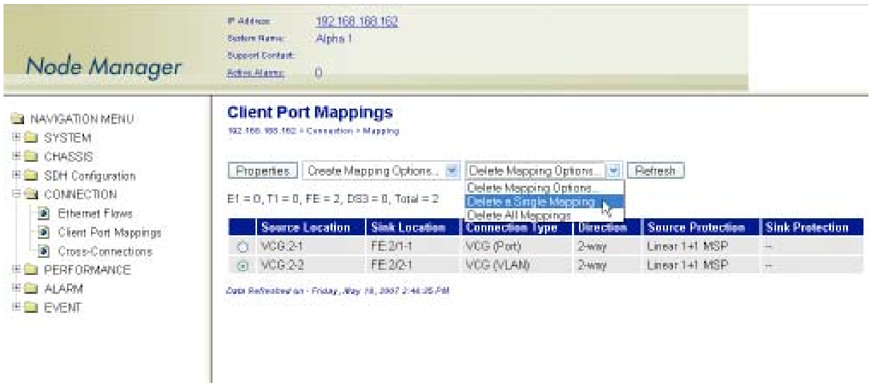
Figure 125. Connecting an Ethernet Flow to a VCG

Removing a Connection

To remove an existing Ethernet flow-to-VCG connection, see Figure 126 and follow these steps:

1. Select an Ethernet port connection on the **Client Port Mappings** page.
2. Select **Delete a Single Mapping** using the **Delete Mapping Options...** scroll-down button.

At this point, the system removes the connection and it is no longer displayed in the table.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Client Port Mappings

192.168.168.162 > Connection > Mapping

E1 = 0, T1 = 0, FE = 2, DS3 = 0, Total = 2

	Source Location	Sink Location	Connection Type	Direction	Source Protection	Sink Protection
○	VCG:2-1	FE:2/1-1	VCG (Port)	2-way	Linear 1+1 MSP	--
●	VCG:2-2	FE:2/2-1	VCG (VLAN)	2-way	Linear 1+1 MSP	--

Data Refreshed on - Friday, May 18, 2007 2:44:25 PM

Figure 126. Removing an Ethernet Flow from a VCG

Ethernet Alarms

The following section describes the process for monitoring alarms that may be present on Ethernet ports and the process of changing the default alarm settings.

Monitoring Port Alarms

Table 71 provides a list of the alarms that the system monitors at the Ethernet port level.

Table 71. Ethernet Port Alarms

Alarm	Description
Ethernet Link Down	Ethernet link is down
Ethernet Buffer Overflow	Buffer has overflowed
Ethernet Loopback	Buffer has overflowed

Note The system declares and displays an alarm condition if a defect persists for 2.5 ± 0.5 seconds. The alarm condition is cleared when the defect is terminated and remains absent for 10 ± 0.5 seconds.

Two LEDs are present for each port on the base system to indicate link status and activity. The LEDs are lit according to the color codes in Table 72.

Table 72. Status LED for Ethernet Ports on the Base System

LED Type	LED Color	LED Is On	LED Is Off
Link	Green	Ethernet link is up	Ethernet link is down
Activity	Amber	Blinks when there is Ethernet traffic on link	No Ethernet traffic on link

To display Ethernet alarms, if present, see Figure 127 and follow these steps:

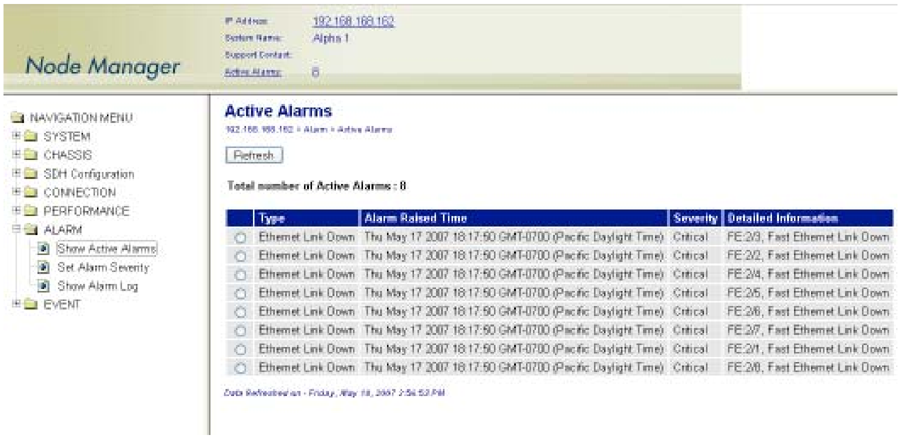
1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Show Active Alarms**.

At this point, the **Active Alarms** page displays all active alarms in the system, including Ethernet alarms, if present. Table 73 describes the fields for each Ethernet alarm entry. The table contains a separate entry for each active Ethernet alarm. Each entry includes the following fields:

Table 73. Table Entries for Active Ethernet Alarms

Table Entry for Active Alarms	Field Value
Type	**Link Down, Buffer Overflow,** or **Loopback**
Alarm Raised Time	Date and time
Severity	Critical, Major, Minor, or Warning
Detailed Information	Location of affected Ethernet port (FE:*slot/port*)

Note The system automatically updates the Active Alarms page every 60 seconds. Click on Refresh if you need to update the table with the most recent active alarm information. Individual table entries automatically clear whenever previously active alarms are no longer present.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 8

Active Alarms

192.168.168.162 > Alarm > Active Alarms

Total number of Active Alarms : 8

	Type	Alarm Raised Time	Severity	Detailed Information
○	Ethernet Link Down	Thu May 17 2007 18:17:50 GMT-0700 (Pacific Daylight Time)	Critical	FE:2/3, Fast Ethernet Link Down
○	Ethernet Link Down	Thu May 17 2007 18:17:50 GMT-0700 (Pacific Daylight Time)	Critical	FE:2/2, Fast Ethernet Link Down
○	Ethernet Link Down	Thu May 17 2007 18:17:50 GMT-0700 (Pacific Daylight Time)	Critical	FE:2/4, Fast Ethernet Link Down
○	Ethernet Link Down	Thu May 17 2007 18:17:50 GMT-0700 (Pacific Daylight Time)	Critical	FE:2/5, Fast Ethernet Link Down
○	Ethernet Link Down	Thu May 17 2007 18:17:50 GMT-0700 (Pacific Daylight Time)	Critical	FE:2/6, Fast Ethernet Link Down
○	Ethernet Link Down	Thu May 17 2007 18:17:50 GMT-0700 (Pacific Daylight Time)	Critical	FE:2/7, Fast Ethernet Link Down
○	Ethernet Link Down	Thu May 17 2007 18:17:50 GMT-0700 (Pacific Daylight Time)	Critical	FE:2/1, Fast Ethernet Link Down
○	Ethernet Link Down	Thu May 17 2007 18:17:50 GMT-0700 (Pacific Daylight Time)	Critical	FE:2/8, Fast Ethernet Link Down

Data Refreshed on - Friday, May 18, 2007 2:56:52 PM

Figure 127. Displaying Ethernet Port Alarms

Changing Port Alarm Default Severities

Table 74 provides the default severities for Ethernet port alarms:

Table 74. Ethernet Line Alarm Default Severities

Monitored Entity	Near-end Alarm	Default Severity
Ethernet port	Link Down	Critical
Ethernet port	Buffer Overflow	Major
Ethernet port	Loopback	Minor

To change the default severity for supported Ethernet alarms, see Figure 128 and follow these steps:

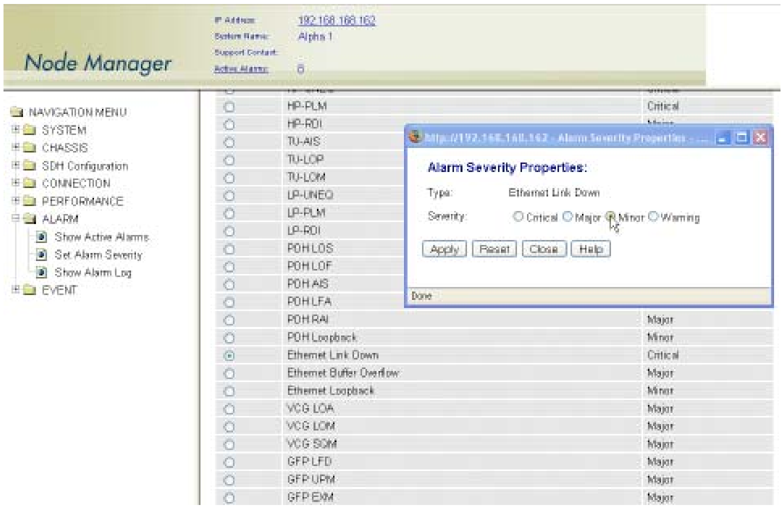
1. Select the **ALARM** folder from the navigation menu.
2. From the expanded **ALARM** folder, select **Set Alarm Severity**.

At this point, the **Alarm Severity** page displays a table with all supported system alarms.

3. Select the table entry containing the Ethernet port alarm **Type** and click on **Change**.
4. In the **Alarm Severity** window, set **Severity** to any desired level (Critical, Major, Minor, or Warning).
5. Click on **Apply** and then on **Close** to close the window.

On the **Alarm Severity** page, the **Severity** for the selected Ethernet port alarm **Type** should now reflect the change in the reported severity level.

Note The change applies to all Ethernet ports within the system.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 6

http://192.168.168.162 - Alarm Severity Properties - ...

Alarm Severity Properties:

Type: Ethernet Link Down

Severity: ○ Critical ○ Major ● Minor ○ Warning

Apply | Reset | Close | Help

○	HP-PLM	Critical
○	HP-RDI	
○	TU-AIS	
○	TU-LOP	
○	TU-LOM	
○	LP-UNEQ	
○	LP-PLM	
○	LP-RDI	
○	POH LOS	
○	POH LOF	
○	POH AIS	
○	POH LFA	
○	POH RAI	Major
○	POH Loopback	Minor
●	Ethernet Link Down	Critical
○	Ethernet Buffer Overflow	Major
○	Ethernet Loopback	Minor
○	VCG LOA	Major
○	VCG LOM	Major
○	VCG SQM	Major
○	GFP LFD	Major
○	GFP UPM	Major
○	GFP EXM	Major

Figure 128. Changing Ethernet Port Alarm Settings

Ethernet Port Statistics

The following section describes the process for displaying current traffic statistics for Ethernet ports.

The system collects performance statistics at the Ethernet port level, as listed in Table 75.

Table 75. Ethernet Port Statistics

Parameter	Monitoring Direction
Octets	Incoming and outgoing
Unicast packets	Incoming and outgoing
Errors	Incoming only
Discards	Incoming only

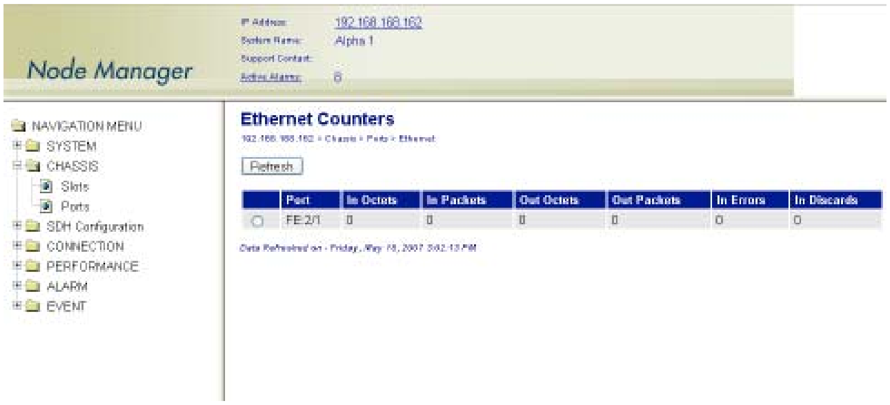
To display the current performance statistics for an Ethernet port, see Figure 129 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports.**
3. On the **Ports** page, select the Ethernet port being monitored and click on **Properties**.

Note The system displays the performance statistics for the selected Ethernet port. The system uses 32-bit counters for all monitored parameters. The window content is not updated automatically as new counts occur. Click on Refresh if you need to update the window content with the most recent count information.

4. Click on **Close** to close the window.

Note You can also display the current performance statistics by clicking on **Show PM** on the **Ports** page after selecting one of the Ethernet ports.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 6

Ethernet Counters

192.168.168.162 > Chassis > Ports > Ethernet

	Port	In Octets	In Packets	Out Octets	Out Packets	In Errors	In Discards
○	FE 2/1	0	0	0	0	0	0

Data Refreshed on - Friday, May 18, 2007 3:02:13 PM

Figure 129. Displaying Ethernet Port Statistics

To display the Ethernet counters for all enabled Ethernet ports, follow these steps:

1. Select the **PERFORMANCE** folder from the navigation menu.
2. From the expanded **PERFORMANCE** folder, select **Counters.**
3. From the expanded **Counters** folder, select **Ethernet**.

At this point, the system displays the performance statistics for all enabled Ethernet ports. The table is empty when no ports are enabled.

Note The system uses 32-bit counters for all monitored parameters.

To clear the counters for a port, select the port entry on the table and then click on **Clear Statistics**.

Note The table content is not updated automatically as new counts occur. Click on **Refresh** if you need to update the table content with the most recent count information.

Ethernet Testing

The following section provides the procedures for enabling and disabling loopback tests for Ethernet ports.

The OS-10 system supports terminal loopback for Ethernet ports. As shown in Figure 130, while the terminal loopback is active, the Ethernet signal is looped back towards the STM-1 interface just before transmission on the Ethernet PHY. The idle sequence is also transmitted on the physical port. Terminal loopback allows the testing of the performance and connectivity for an Ethernet service across the SDH network.

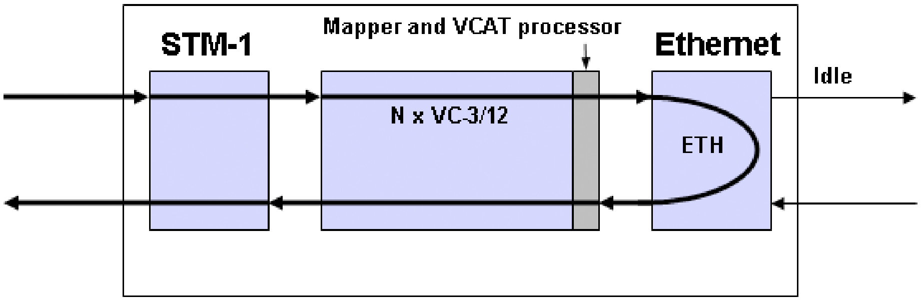


Figure 130. Ethernet Terminal Loopback

To start an Ethernet terminal loopback test, see Figure 131 on page 213 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports.**
3. On the **Ports** page, select the Ethernet port being tested and click on **Properties**.
4. In the **Port Properties** window, click on **Start Terminal Loopback.**

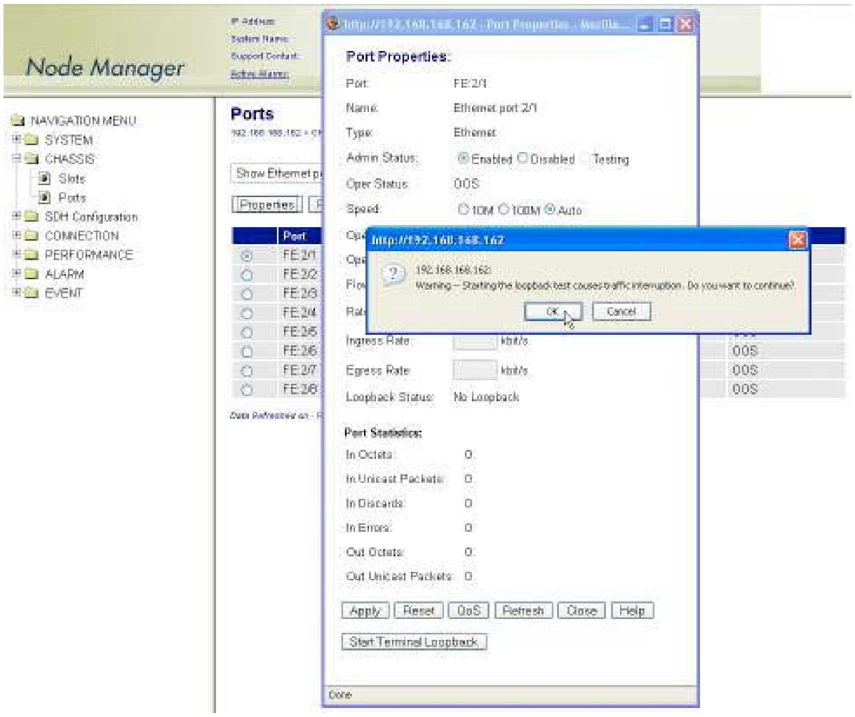
A warning window opens to alert you to the start of the loopback test. Click on **OK** to continue or **Cancel** to cancel the request.

WARNING

Starting an Ethernet terminal loopback causes traffic disruption if the Ethernet port is already connected to a VCG.

Loopback Status on the **Port Properties** window changes to **Terminal Loopback Active**. **Admin Status** for the port changes to **Testing.**

5. Click on **Close** to close the **Port Properties** window.



http://192.168.168.162 - Port Properties - Mozilla...

Port Properties:

Port: FE 2/1

Name: Ethernet port 2/1

Type: Ethernet

Admin Status: ● Enabled ○ Disabled Testing

Oper Status: OOS

Speed: ○ 10M ○ 100M ● Auto

Ingress Rate: kbit/s

Egress Rate: kbit/s

Loopback Status: No Loopback

Port Statistics:

In Octets: 0

In Unicast Packets: 0

In Discards: 0

In Errors: 0

Out Octets: 0

Out Unicast Packets: 0

http://192.168.168.162

192.168.168.162

Warning – Starting the loopback test causes traffic interruption. Do you want to continue?

Figure 131. Activating Ethernet Port Terminal Loopback

Chapter 7 High-Density E1 Expansion Module

Chapter contents

Introduction

As an option, the system allows the installation of a high-density E1 (HD-E1) expansion module for applications requiring additional E1 drop capacity. Figure 132 provides a front-side view of the module.

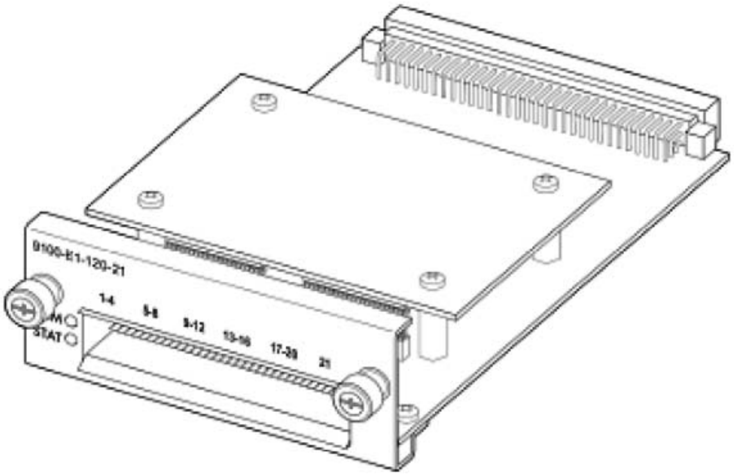


Figure 132. HD-E1 Module

The HD-E1 expansion module has 21 E1 interfaces and supports 120-ohm (balanced) and 75-ohm (unbalanced) terminations as factory-installed options. E1 signals comply with the specifications in G.703. Table 76 shows the product codes that identify which type of termination is supported. The product code is located on the front plate of the module.

Table 76. Product Codes for the HD-E1 Module

Code	Interface	Termination
9100-E1-075-21	21 E1	75-ohm
9100-E1-120-21	21 E1	120-ohm

The module weighs approximately 0.2 kg (0.5 lbs) and has the following dimensions: 38 x 101 x 167 mm (height x weight x depth). E1 ports are connected to individual TU-12 time slots using asynchronous mapping into VC-12 containers, as specified in ITU-T Recommendation G.707.

The module uses a high-density Future Bus connector on the front panel. The connector is divided into six sections. Each section supports bidirectional transmission of four E1 ports. Connector section 6, however, supports only one E1 port for a combined total of 21 E1 ports. Table 77 provides the port assignments for E1 ports on the Future Bus connector.

Table 77. E1 Port Assignments for Future Bus Connector Sections

Connector Section	E1 Ports
1	1-4
2	5-8
3	9-12
4	13-16
5	17-20
6	21

Each Future Bus connector section has 24 pins. Table 78 shows the pin layout of a connector section. The table columns represent the physical location of the connector section pins when viewed from the front.

Table 78. Pin Assignment in a Future Bus Connector Section

Connector Section Pin Column					
1	2	3	4	5	6
TXP-1	TXN-2	TXP-2	TXN-3	TXP-3	TXN-4
TXN-1	–	–	–		TXP-4
RXN-1	–	–	–		RXP-4
RXP-1	RXN-2	RXP-2	RXN-3	RXP-3	RXN-4

Note TXP and TXN correspond to the positive (tip) and negative (ring) pins for the transmit signal. RXP and RXN correspond to the receive side of the signal.

For physical interconnection between the module and other equipment, you need special cables. These cables have to be ordered separately, and the type and length of each cable has to be specified at the moment that you order the module.

- For 75-ohm interfaces, each cable supports connectivity for four E1 ports. The cable provides eight BNC connectors (four transmit and receive pairs) on one end and a single Future Bus plug on the other end. You can connect the Future Bus plug to any available connector section on the module.
- For 120-ohm interfaces, each cable supports connectivity for four E1 ports. One side of the cable contains twisted-pair wires (four transmit and receive pairs) that you can use for direct termination on an MDF (wire-wrap) or four RJ-48 connectors. The size of the twisted-pair cables is 28 AWG (or 4 mm). The cable has a single Future Bus plug on the other end. You can connect the Future Bus plug to any available connector section on the module. You can also bind together three cables and terminate the E1 signals on a single RJ-21 Telco connector (12 transmit and receive pairs). Table 79 on page 217 provides the connector pin-out assignments for 12 E1 ports using the RJ-21 Telco connector termination. For this 12-port E1 cable configuration, it is recommended that you connect the three Future Bus plugs to three consecutive connector sections, either in sections 1 through 3 or 4 through 6.

Table 79. Pin Assignments for E1 Ports 1–12 and 13–21 Using a 50-Pin Telco Connector

E1 Port	Tip	Connector Pins		Ring
1	TX	1	26	TX
	RX	2	27	RX
2	TX	3	28	TX
	RX	4	29	RX
3	TX	5	30	TX
	RX	6	31	RX
4	TX	7	32	TX
	RX	8	33	RX
5	TX	9	34	TX
	RX	10	35	RX
6	TX	11	36	TX
	RX	12	37	RX
7	TX	13	38	TX
	RX	14	39	RX
8	TX	15	40	TX
	RX	16	41	RX
9	TX	17	42	TX
	RX	18	43	RX
10	TX	19	44	TX
	RX	20	45	RX
11	TX	21	46	TX
	RX	22	47	RX
12	TX	23	48	TX
	RX	24	49	RX
	–	25	50	–
13	TX	1	26	TX
	RX	2	27	RX
14	TX	3	28	TX
	RX	4	29	RX
15	TX	5	30	TX
	RX	6	31	RX
16	TX	7	32	TX
	RX	8	33	RX
17	TX	9	34	TX
	RX	10	35	RX
18	TX	11	36	TX
	RX	12	37	RX
19	TX	13	38	TX
	RX	14	39	RX
20	TX	15	40	TX
	RX	16	41	RX
21	TX	17	42	TX
	RX	18	43	RX
	–	19	44	–
	–	20	45	–
	–	21	45	–
	–	22	46	–
	–	23	48	–
	–	24	49	–
	–	25	50	–

Installing the HD-E1 Module

The HD-E1 module supports hot swapping. You can insert the module into or remove it from any available expansion slot of the chassis while the system is powered on and carrying traffic.

To install the HD-E1 module, see Figure 133 and follow these steps:

1. Remove the front plate cover for the slot in which you wish to install the module. Turn each mounting screw in a counterclockwise direction until the cover is fully released from the chassis.
2. Remove the HD-E1 module from the ESD bag, and place it on a flat, clean and dry surface (use a grounded antistatic mat, if possible).

Note Set the ESD bag aside for reuse in case you need it to replace and return the module in the future.

3. Align the module with the card guides inside the slot and slide the module slowly into the slot.

CAUTION

Be careful to maintain the alignment along the card cage guide rail axis as you insert the module. Do not rotate or pull the module up or down during the insertion procedure or you may risk breaking the module. Make sure that the mezzanine board clears the hole plates on each side of the slot aperture.

4. Push the front plate (gently applying force on each side of the plate at the same height as the guide rail) until the module is securely snapped in place. The front plate should be flush with the front panel of the OS-10 system.
5. Secure the module to the chassis by turning the two mounting screws on the front panel of the module in a clockwise direction.

At this point, use the OnSight Device Manager to set the **Administrative Type** for the slot in which the module resides to **21-port E1 expansion module**. The STAT LED of the HD-E1 module becomes a solid green light when the **Administrative Status** of the module is enabled and **Operational Status** is in service (IS).

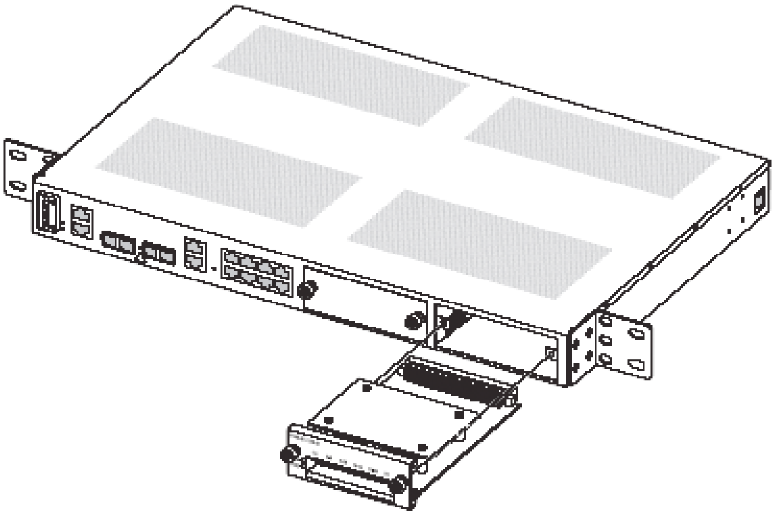


Figure 133. Installing the HD-E1 Module

Provisioning the HD-E1 Module

To provision the HD-E1 module, see Figure 134 on page 220 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Slots**.
3. On the **Slots** page, check that the **Status** for the slot in which the module resides is **Full**.

> **Note** On the **Slots** page, the **Status** indicates the presence of a module in the expansion slots. When a module is physically present and properly inserted in slot 2 or 3, the table entry shows **Full** for that slot. Otherwise, the table entry shows **Empty**.

4. Check that the **Operational Type** for the slot shows: **21-port E1 expansion module**.

> **Note** The **Operational Type** indicates the type of module in the slot. The table entry shows **21-port E1 expansion module** when the system has software access and control for the HD-E1 module. Otherwise, the entry shows **Unknown**, even when the module is physically present in the slot.

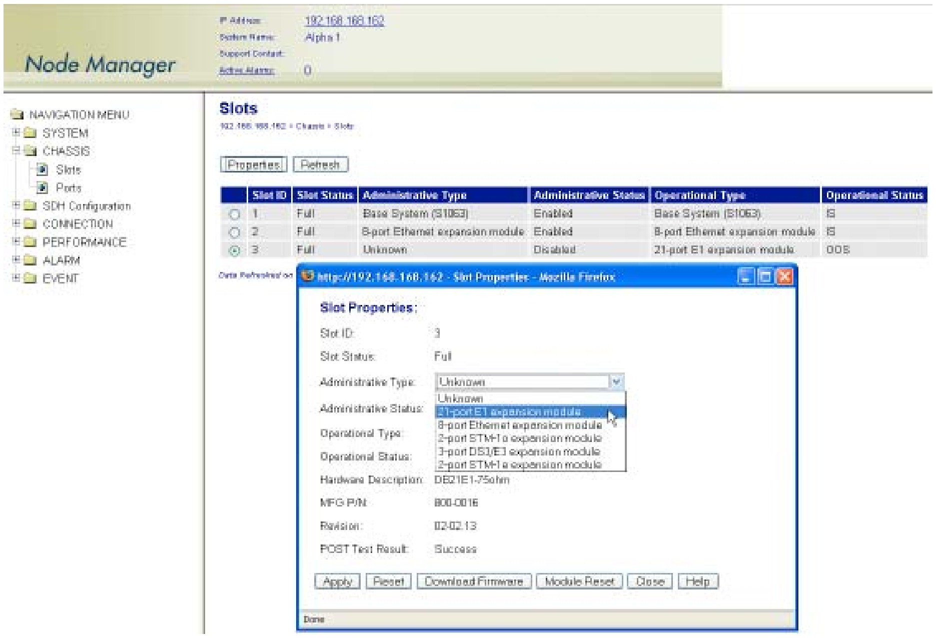
> **Note** When the **Operational Type** is **Unknown** and the module is securely installed in the chassis, the module may need replacement. Consult your nearest support center or systems engineer servicing the system for technical support.

5. Select the **Slot ID** for the slot in which the module resides, and click on **Properties**.
6. In the **Slot Properties** window, set the **Administrative Type** to **21-port E1 expansion module** using the scroll-down button.
7. Set the **Administrative Status** to **Enabled**.
8. Click on Apply for the settings to take effect.

> **Note** You can also use the **Slot Properties** window to check the inventory for the module, including the hardware description, manufacturing part number (MFG P/N) and revision. You can also use the **Slot Properties** window to verify that the module completed the POST.

9. Click on **Close** to close the window and finish this task.

At this point, the module is now ready for the provisioning of E1 services using the OnSight Device Manager or NMS.


Node Manager
NAVIGATION MENU
SYSTEM
CHASSIS
Slots
Ports
SDH Configuration
CONNECTION
PERFORMANCE
ALARM
EVENT
Properties
Refresh
Data Refreshed on
http://192.168.168.162 - Slot Properties - Mozilla Firefox
Unknown
21-port E1 expansion module
8-port Ethernet expansion module
2-port STM-1 o expansion module
3-port DS3/E3 expansion module
2-port STM-1 e expansion module
Apply
Reset
Download Firmware
Module Reset
Close
Help
Done

IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Slots

192.168.168.162 > Chassis > Slots

	Slot ID	Slot Status	Administrative Type	Administrative Status	Operational Type	Operational Status
○	1	Full	Base System (S1063)	Enabled	Base System (S1063)	IS
○	2	Full	8-port Ethernet expansion module	Enabled	8-port Ethernet expansion module	IS
●	3	Full	Unknown	Disabled	21-port E1 expansion module	OOS

Slot Properties:

Slot ID: 3
Slot Status: Full
Administrative Type: Unknown
Administrative Status:
Operational Type:
Operational Status:
Hardware Description: DB21E1-75ohm
MFG P/N: 800-0016
Revision: 02-02.13
POST Test Result: Success

Figure 134. Provisioning the HD-E1 Module

Note The system displays all E1 ports in slot 2 and slot 3 when the **Administrative Type** for those slots is set to **Enabled**. The module need not be physically present in the slot for the system to display the ports on the Ports page.

You can preconfigure E1 port mappings before the module is physically present in the slot.

The system maintains all existing E1 expansion port mappings in the **Client Port Mappings** connection table even after physical removal of the module from the slot.

CAUTION

Save the system configuration to prevent the loss of the module settings if a system reboot occurs

Module Alarms

Table 80 provides a list of the alarms that the system monitors for the HD-E1 module.

Table 80. Module Alarms

Alarm Name	Default Severity	Occurs when the . . .
Card Initialization Failed	Critical	Module fails the POST.
Card Failure	Critical	System fails to access the hardware correctly.
Card Missing	Critical	System fails to access the hardware correctly.
Card Mismatched	Critical	Administrative and operational types are different.
Card Mismatched	Major	Software cannot support the current version of hardware.

The alarm (ALM) status LED indicates the presence of an active alarm condition of any severity level on any of the 21 E1 ports on the HD-E1 module. The LED is lit according to the color codes in Table 81.

Table 81. ALM (Alarm Status) LED for the HD-E1 Module

LED Color	Description
Green	No alarm is present on any port.
Amber	An alarm is present on one or more ports.
Off	All E1 ports are disabled.

Timing Features on the HD-E1 Module

The following section describes the timing features of the HD-E1 module. The module supports all the E1 timing functions, except for Sync Out. Table 82 notes the differences between the timing features supported by the E1 ports on the OS1052 and OS1063 base systems and the HD-E1 expansion module.

Table 82. Timing Feature Differences for E1 Ports on the OS-10 and the HD-E1 Module

E1 Ports in the	E1 Line Timing Is On	Sync In Is On	Sync Out Is On
OS1052 base system	Ports 7–8	Ports 7–8	Ports 7–8
OS1063 base system	Ports 20-21	Ports 20-21	Ports 20-21
HD-E1 module	Ports 20-21	Ports 20-21	–

Derived Timing from E1 Line

To configure the system to use E1 ports 20 and 21 from a HD-E1 module as the primary and secondary references for synchronization using line timing, follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Timing & Sync**.
3. On the **Timing & Synchronization** page, select **Auto: E1 port 2/20**, **port 2/21** using the **Timing Mode – Primary/Secondary Source** scroll-down button.
4. Click on **Apply** for the changes to take effect.

Note The system does not allow the change of the timing mode directly from one primary-and secondary-timing-source pair to another. You must first change the timing mode to Internal and then to **Auto: E1 port 2/20, port 2/21**.

- By default, E1 ports 20 and 21 are configured for carrying regular E1 traffic. In the "traffic" mode, the system uses the derived 2.048-MHz clock from the E1 lines as timing references for synchronization. You can view the current port signal mode in the **Ports** page or **Port Properties** window for E1 ports 20 and 21.

External Timing Inputs

To configure E1 ports 20 and 21 as external timing inputs for synchronization (Sync In), follow these steps:

1. Go through the steps in "Configuring a Port for Synchronization" on page 150, but use **E1:slot/20** (instead of E1:1/7) and **E1:slot/21** (instead of E1:1/8) for the procedure. Change the port signal mode for these ports to **Sync In**.

Note The slot refers to the expansion slot in which the module resides. The **Port Properties** window for E1 ports 20 and 21 provides the same configuration options as that for E1:1/7 and E1:1/8.

2. Go through the steps in "Derived Timing from E1 Line" on page 221 to configure the system to use E1:slot/20 and E1:slot/21 as the timing references for synchronization.

Retiming Mode

The HD-E1 module supports a retiming function for E1 ports 1-8, individually. In the regular mode of operation, the module uses the recovered clock from the demapped E1 signal for transmission into the physical E1 line. In the retiming mode, however, the module uses the system clock to transmit the E1 signal. You may use the retiming mode to distribute system timing to other equipment (such as PBXs or BTSs) that connects to the OS-10 at the E1 line level using the HD-E1 module.

To enable the retiming feature for E1 ports 1-8 in the HD-E1 module, follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Ports**.
3. On the **Ports** page, select **E1:*slot/port*** and click on **Properties**.

Note The retiming function of an HD-E1 module in slot 2 or 3 is available only for E1 port numbers 1-8.

4. In the **Port Properties** window, set **Retiming** to **Enabled**.
5. Click on **Apply** and then on **Close** to close the window.

Downloading Expansion Module Firmware

To download and install new firmware into the expansion modules, see Figure 135 on page 224 and follow these steps:

Note This procedure applies only when the system is equipped with one or two expansion modules and a new firmware upgrade is required.

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Slots**.
3. On the **Slots** page, select the expansion module that requires the new firmware and click on Properties. Slot 2 and slot 3 are the respective slots for expansion modules 1 and 2. Slot 1 corresponds to the base OS-10 system.
4. On the **Slot Properties** page, click on **Download Firmware.**
5. In the **Download Expansion Module Firmware** window, set **Transfer Protocol** to **FTP** or **TFTP**. FTP is the default transfer protocol. FTP and TFTP work on Windows, UNIX, and Linux servers.
6. Type the **Host Pathname** to indicate the name of the firmware image file to be retrieved and its location within the host server.

Note You must specify either the full or relative pathname from the server root directory to indicate the location of the firmware image file. The file name for the firmware image must contain the .img extension.

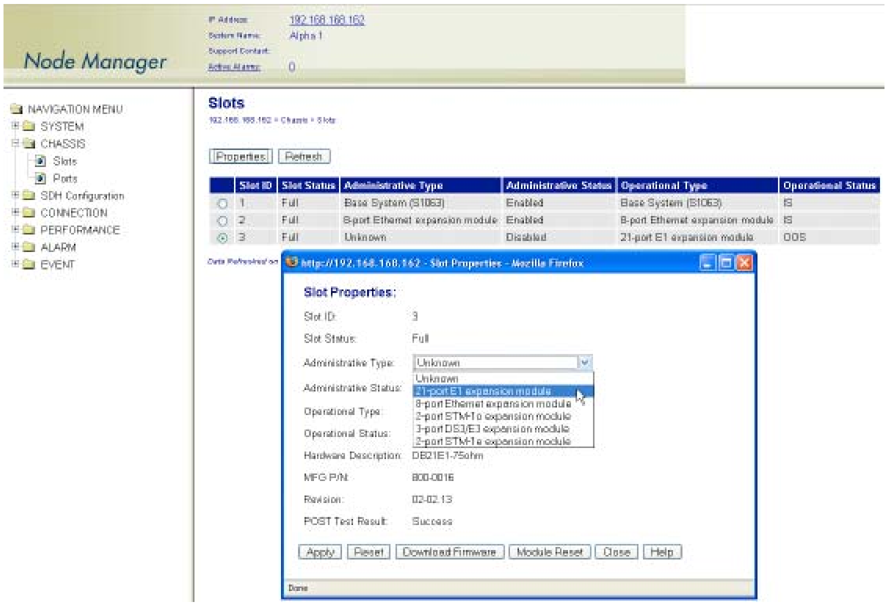
7. Type the **Server IP Address** of the host server containing the firmware image file.
8. Type the **User Name** and **Password** for secure access to the file. In this step, you must enter the user name and password, as demanded by the server access permission.
9. Click on **Apply** to initiate the file transfer between the server and OS-10 system.

At this point, the system indicates the download progress in **Transfer Progress** (%). The firmware download operation may take a few minutes to complete. The new firmware takes effect after completion of the next system reboot. You can also activate the new firmware immediately by clicking on **Module Reset** at the bottom of the window.

WARNING **Make sure that the Transfer Result indicates Success and transfer is 100-percent complete before rebooting the system or resetting the module. If the transfer result is Fail, keep trying to download the firmware until the result is Success. In addition, do not power cycle the system or reset the module while the download is in progress. Rebooting the system or resetting the module with a corrupted firmware image makes the module permanently inoperative and requires module replacement.**

CAUTION

After installation of the new firmware is complete, check that the **Slot Properties** window indicates a change in the firmware **Revision** field (that is, from the old firmware revision code to the new code). If the firmware revision code remains as before, click on the **Module Reset** button until **Revision** indicates a change to the new code. Otherwise, the new firmware is not installed and operational.



Node Manager

IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Slots

192.168.168.162 » Chassis » Slots

	Slot ID	Slot Status	Administrative Type	Administrative Status	Operational Type	Operational Status
○	1	Full	Base System (S1063)	Enabled	Base System (S1063)	IS
○	2	Full	8-port Ethernet expansion module	Enabled	8-port Ethernet expansion module	IS
●	3	Full	Unknown	Disabled	21-port E1 expansion module	OOS

Data Refreshed on

http://192.168.168.162 - Slot Properties - Mozilla Firefox

Slot Properties:

Slot ID: 3
Slot Status: Full
Administrative Type: Unknown
Administrative Status:
Operational Type:
Operational Status:
Hardware Description: DB21E1-75ohm
MFG P/N: 800-0016
Revision: 02-02.13
POST Test Result: Success

Unknown
21-port E1 expansion module
8-port Ethernet expansion module
2-port STM-1o expansion module
3-port DS3/E3 expansion module
2-port STM-1e expansion module
Apply
Reset
Download Firmware
Module Reset
Close
Help
Done

Figure 135. Download Firmware into the Expansion Modules

Chapter 8 High-Density Ethernet Expansion Module

Chapter contents

Introduction

As an option, the system allows the installation of a high-density Ethernet (HD-ENET) expansion module for applications that require access to additional Ethernet ports together with enhanced virtual concatenation (VCAT) and flexible Layer 2 functions. Figure 136 provides a front-side view of the module.

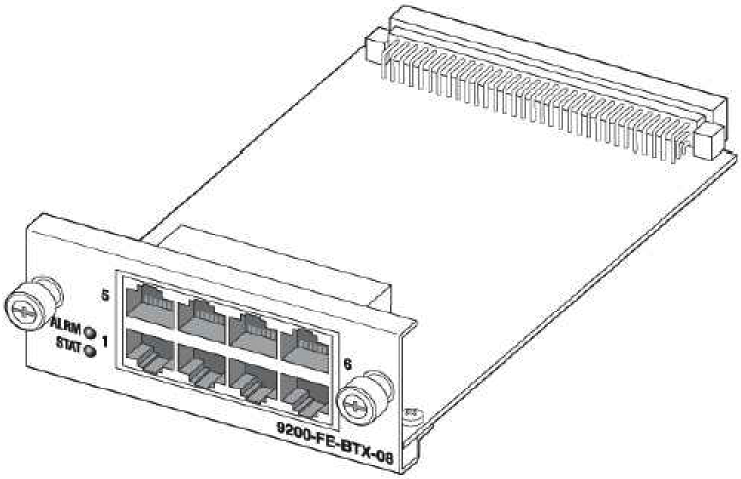


Figure 136. HD-ENET Module

The HD-ENET module has eight Ethernet 10/100BASE-TX interfaces. The module weighs approximately 0.2 kg (0.5 lbs) and has the following dimensions: 38 x 101 x 167 mm (height x weight x depth).

Ethernet traffic is mapped into VCAT Groups (VCGs) using GFP encapsulation, as specified in ITU-T Recommendations G.7041/Y.1303 and G.707. The module supports up to 16 VCGs.

The Ethernet ports comply with the following standards:

- IEEE 802.3u (PHY)
- IEEE 802.3 (MAC)
- IEEE 802.3x (flow control)

The module supports Ethernet frames in the following range: 64 to 1,600 bytes.

Note The Ethernet ports on the base OS1052 system support jumbo frames up to 9,600 bytes.

Table 83 provides the cabling specifications for the Ethernet ports.

Table 83. Ethernet Port Cabling Specifications

Cable	Specification
Connector	RJ-45
Type	Category 5
Reach	100 m

Table 84 provides the pin assignment for the Ethernet RJ-45 connector.

Table 84. Ethernet Port Pin Assignment (RJ-45 Connector)

Signal Name	Description	RJ-45 Pin
RXN	Receive ring	6
RXP	Receive tip	3
TXN	Transmit ring	2
TXP	Transmit ring	1

Installing the HD-ENET Module

The HD-ENET module supports hot swapping. You can insert the module into or remove it from any available expansion slot of the chassis while the system is powered on and carrying traffic. This process does not result in the loss or disruption of existing traffic on the system.

To install the HD-ENET module, see Figure 137 on page 228 and follow these steps:

Note Although not required, you may power down the system before starting the module insertion procedure.

1. Remove the front plate cover for the slot in which you wish to install the module. Turn each mounting screw in a counterclockwise direction until the cover is fully released from the chassis.
2. Remove the HD-ENET module from the ESD bag and place it on a flat, clean, and dry surface (use a grounded antistatic mat, if possible).

Note Set the ESD bag aside for reuse in case you need it to replace and return the module in the future.

3. Align the module with the card guides inside the slot and slide the module slowly into the slot.

CAUTION

Be careful to maintain the alignment along the card cage guide rail axis as you insert the module. Do not rotate or pull the module up or down during the insertion procedure, or you may risk breaking the module.

4. Push the front plate (gently applying force on each side of the plate at the same height as the guide rail) until the module is securely snapped in place. The front plate should be flush with the front panel of the OS-10 system.
5. Secure the module to the chassis by turning the two mounting screws on the front panel of the module in a clockwise direction.

The STAT LED of the HD-ENET module becomes a solid amber light for about 10 seconds after the system detects the module. At this point, use the OnSight Device Manager to set the **Administrative Type** for the slot in which the module resides to **8-port Ethernet expansion module**. The STAT LED of the module becomes a solid green light when the **Administrative Status** of the module is enabled and the **Operational Status** is in service (**IS**).

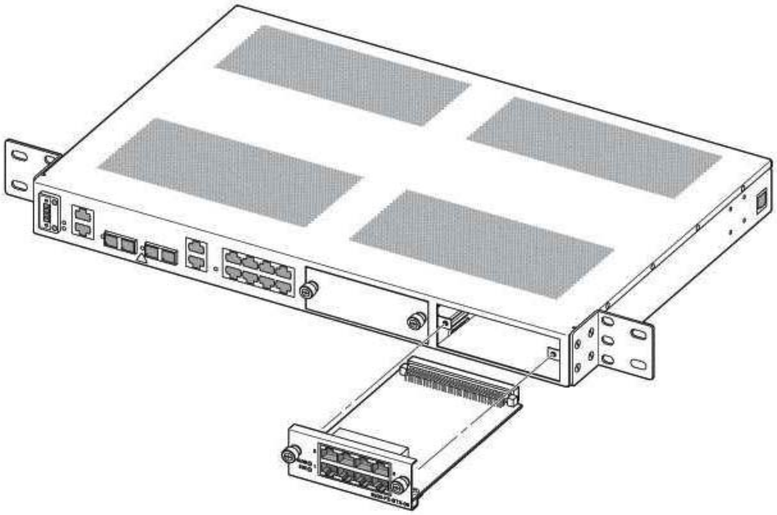


Figure 137. Installing the HD-ENET Module

Provisioning the HD-ENET Module

To provision the HD-ENET module, see Figure 138 on page 229 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Slots**.
3. On the **Slots** page, check that the **Status** for the slot in which the module resides is **Full**.

> **Note** On the **Slots** page, the **Status** indicates the presence of a module in the expansion slots. When a module is physically present and properly inserted in slot 2 or 3, the table entry shows **Full** for that slot. Otherwise, the table entry shows **Empty**.

4. Check that the **Operational Type** for the slot shows: **8-port Ethernet expansion module.**

> **Note** The **Operational Type** indicates the type of module in the slot. The table entry shows **8- port Ethernet expansion module** when the system has software access and control for the HDENET module. Otherwise, the entry shows **Unknown** even when the module is physically present in the slot.

> **Note** When the **Operational Type** is **Unknown** and the module is securely installed in the chassis, the module may need replacement. Consult your nearest support center or systems engineer servicing the system for technical support.

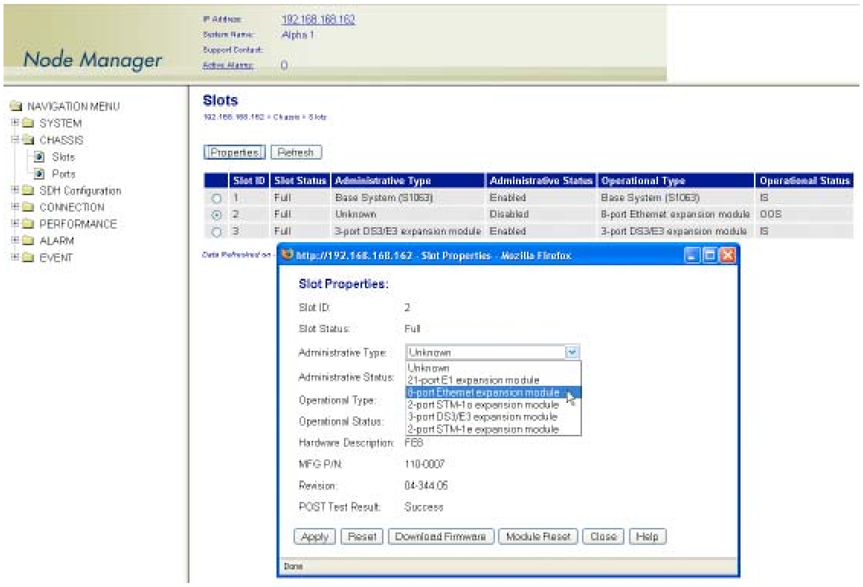
5. Select the **Slot ID** for the slot in which the module resides, and click on **Properties**.

6. In the **Slot Properties** window, set the **Administrative Type** to **8-port Ethernet expansion module** using the scroll-down button.
7. Set the **Administrative Status** to **Enabled**.
8. Click on **Apply** for the settings to take effect.

Note You can also use the Slot Properties window to check the inventory for the module, including the hardware description, manufacturing part number (MFG P/N), and revision. You can also use the **Slot Properties** window to verify that the module completed the POST.

9. Click on **Close** to close the window and finish this task.

At this point, the module is now ready for the provisioning of Ethernet services using the OnSight Device Manager or NMS.


Node Manager
NAVIGATION MENU
SYSTEM
CHASSIS
Slots
Ports
SDH Configuration
CONNECTION
PERFORMANCE
ALARM
EVENT
Properties
Refresh
Data Refreshed on
http://192.168.168.162 - Slot Properties - Mozilla Firefox
Unknown
21-port E1 expansion module
8-port Ethernet expansion module
2-port STM-1 o expansion module
3-port DS3/E3 expansion module
2-port STM-1 e expansion module
Apply
Reset
Download Firmware
Module Reset
Close
Help
Done

IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Slots

192.168.168.162 > Chassis > Slots

	Slot ID	Slot Status	Administrative Type	Administrative Status	Operational Type	Operational Status
○	1	Full	Base System (S1063)	Enabled	Base System (S1063)	IS
●	2	Full	Unknown	Disabled	8-port Ethernet expansion module	OOS
○	3	Full	3-port DS3/E3 expansion module	Enabled	3-port DS3/E3 expansion module	IS

Slot Properties:

Slot ID: 2
Slot Status: Full
Administrative Type: Unknown
Administrative Status:
Operational Type:
Operational Status:
Hardware Description: FE8
MFG P/N: 110-0007
Revision: 04-344.05
POST Test Result: Success

Figure 138. Provisioning the HD-ENET Module

The system displays all Ethernet ports in slot 2 and slot 3 when the Administrative Type for those slots is set to Enabled. The module need not be physically present in the slot for the system to display the ports on the Ports page.

You can preconfigure Ethernet port mappings before the module is physically present in the slot.

The system maintains all existing Ethernet expansion port mappings in the Client Port Mappings connection table even after physical removal of the module from the slot.

CAUTION

Save the system configuration to prevent the loss of the module settings if a system reboot occurs.

Module Alarms

The HD-ENET module supports the same alarms as the HD-E1 module. Table 80 on page 221 provides a list of the alarms that the system monitors for the HD-ENET module.

A single bicolor LED is present for each port on the module to indicate both link status and activity. The LED is lit according to the color codes in Table 85.

Table 85. Status LED for Ethernet Ports on the HD-ENET Module

LED Is On	LED Is Off
Solid green when link is up and there is no Ethernet traffic on link	Ethernet link is down
Blinks amber when there is Ethernet traffic on link	

Figure 139 shows the location of the LEDs associated with each port on the module.

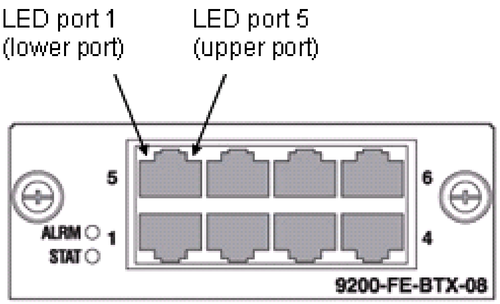


Figure 139. Location of LEDs for Ethernet Ports on the HD-ENET Module

The ALM (alarm status) LED indicates the presence of an active alarm condition of any severity level on any of the eight Ethernet ports on the HD-ENET module. The LED is lit according to the color codes in Table 86.

Table 86. ALM (Alarm Status) LED for the HD-ENET Module

LED Color	Description
Green	No alarm is present on any port.
Amber	An alarm is present on one or more ports.
Off	All Ethernet ports are disabled.

Downloading Expansion Module Firmware

The system supports the downloading and installation of new firmware in the HD-ENET module. The procedure is the same as that for the HD-E1 module (see "Downloading Expansion Module Firmware" on page 223).

The HD-ENET module must be in firmware revision 344.05 to support the LCAS functions in Release 4.2 and above. The system uses the Revision field in the Slot Properties window (see Figure 138 on page 229) to display the firmware revision for the HD-ENET module that resides in the slot.

Chapter 9 High-Density DS3/E3 Expansion Module

Chapter contents

Introduction

As an option, the system allows the installation of a high-density DS3/E3 expansion module for applications that require access and transport of DS3/E3 signals. Figure 140 provides a front view of the module.

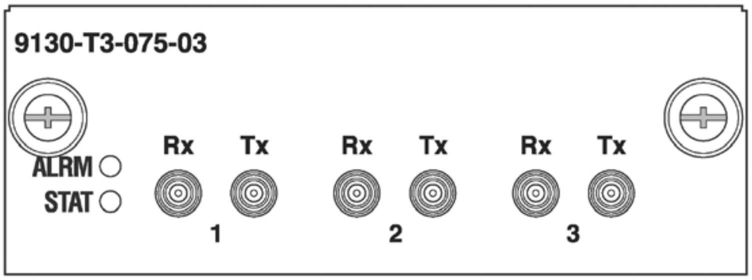


Figure 140. DS3/E3 Module

The DS3/E3 module has three dual-rate DS3/E3 interfaces. Each port can be configured individually for operation at DS3 or E3 rate. The module weighs approximately 0.2 kg (0.5 lbs) and has the following dimensions: 38 x 101 x 167 mm (height x weight x depth).

Installing the DS3/E3 Module

The DS3/E3 module supports hot swapping. You can insert the module into or remove it from any available expansion slot of the chassis while the system is powered on and carrying traffic. This process does not result in the loss or disruption of existing traffic on the system.

To install the DS3/E3 module, see Figure 141 on page 233 and follow these steps:

Note Although not required, you may power down the system before starting the module insertion procedure.

1. Remove the front plate cover for the slot in which you wish to install the module. Turn each mounting screw in a counterclockwise direction until the cover is fully released from the chassis.
2. Remove the DS3/E3 module from the ESD bag and place it on a flat, clean, and dry surface (use a grounded antistatic mat, if possible).

Note Set the ESD bag aside for reuse in case you need it to replace and return the module in the future.

3. Align the module with the card guides inside the slot and slide the module slowly into the slot.

CAUTION Be careful to maintain the alignment along the card cage guide rail axis as you insert the module. Do not rotate or pull the module up or down during the insertion procedure, or you may risk breaking the module.

4. Push the front plate (gently applying force on each side of the plate at the same height as the guide rail) until the module is securely snapped in place. The front plate should be flush with the front panel of the OS-10 system.

5. Secure the module to the chassis by turning the two mounting screws on the front panel of the module in a clockwise direction.

The STAT LED of the DS3/E3 module becomes a solid amber light for about 10 seconds after the system detects the module. At this point, use the OnSight Device Manager to set the **Administrative Type** for the slot in which the module resides to **3-port DS3/E3 expansion module**. The STAT LED of the module becomes a solid green light when the **Administrative Status** of the module is enabled and the **Operational Status** is in service (**IS**).

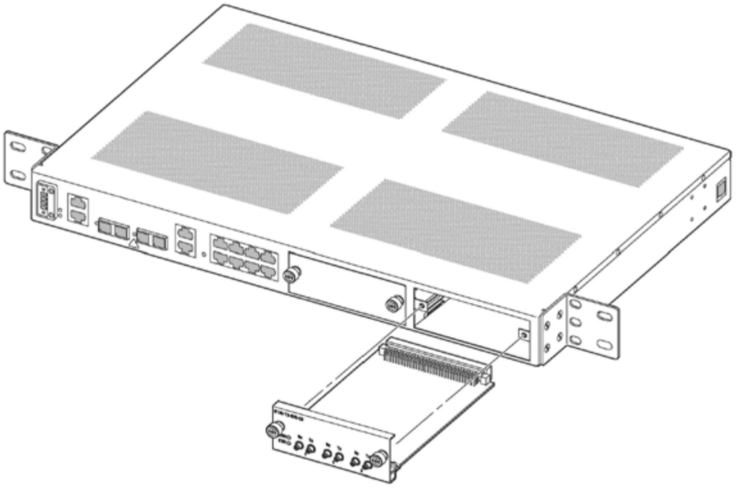


Figure 141. Installing the DS3/E3 Module

Provisioning the DS3/E3 Module

To provision the DS3/E3 module, see Figure 142 on page 234 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Slots**.
3. On the **Slots** page, check that the Status for the slot in which the module resides is **Full**.

Note On the **Slots** page, the **Status** indicates the presence of a module in the expansion slots. When a module is physically present and properly inserted in slot 2 or 3, the table entry shows **Full** for that slot. Otherwise, the table entry shows **Empty.**

4. Check that the **Operational Type** for the slot shows: **3-port DS3/E3 expansion module**.

Note The **Operational Type** indicates the type of module in the slot. The table entry shows **3-port DS3/E3 expansion module** when the system has software access and control for the DS3/E3 module. Otherwise, the entry shows **Unknown** even when the module is physically present in the slot.

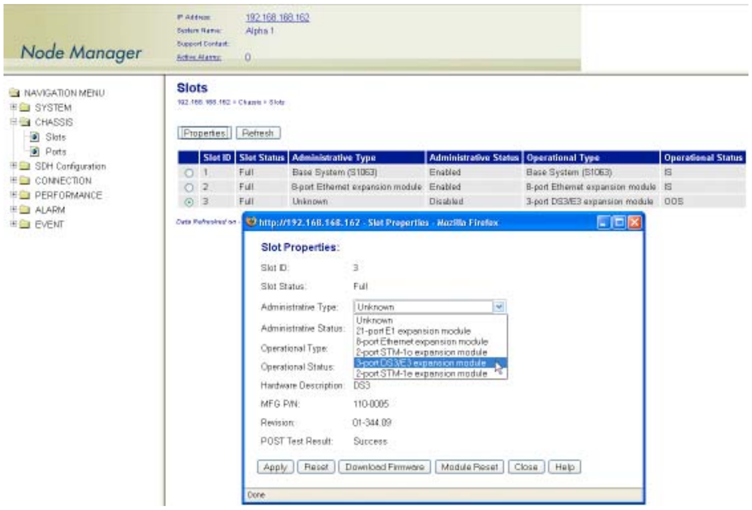
Note When the **Operational Type** is **Unknown** and the module is securely installed in the chassis, the module may need replacement. Consult your nearest support center or systems engineer servicing the system for technical support.

5. Select the **Slot ID** for the slot in which the module resides, and click on **Properties**.
6. In the **Slot Properties** window, set the **Administrative Type** to **3-port DS3/E3 expansion module** using the scroll-down button.
7. Set the **Administrative Status** to **Enabled**.
8. Click on **Apply** for the settings to take effect.

Note You can also use the Slot Properties window to check the inventory for the module, including the hardware description, manufacturing part number (MFG P/N), and revision. You can also use the Slot Properties window to verify that the module completed the POST.

9. Click on **Close** to close the window and finish this task.

At this point, the module is now ready for the provisioning of DS3/E3 services using the OnSight Device Manager or NMS.



	Slot ID	Slot Status	Administrative Type	Administrative Status	Operational Type	Operational Status
○	1	Full	Base System (S1063)	Enabled	Base System (S1063)	IS
○	2	Full	8-port Ethernet expansion module	Enabled	8-port Ethernet expansion module	IS
●	3	Full	Unknown	Disabled	3-port DS3/E3 expansion module	OOS

Slot Properties:

Slot ID: 3
Slot Status: Full
Administrative Type: Unknown
Administrative Status:
Operational Type:
Operational Status:
Hardware Description: DS3
MFG P/N: 110-0005
Revision: 01-344.09
POST Test Result: Success

Unknown
21-port E1 expansion module
8-port Ethernet expansion module
2-port STM-1o expansion module
3-port DS3/E3 expansion module
2-port STM-1e expansion module

Figure 142. Provisioning the DS3/E3 Module

The system displays all DS3/E3 ports in slot 2 and slot 3 when the Administrative Type for those slots is set to Enabled. The module need not be physically present in the slot for the system to display the ports on the Ports page.

You can preconfigure DS3/E3 port mappings before the module is physically present in the slot.

The system maintains all existing DS3/E3 expansion port mappings in the Client Port Mappings connection table even after physical removal of the module from the slot.

CAUTION

Save the system configuration to prevent the loss of the module settings if a system reboot occurs.

Module Alarms

The DS3/E3 module supports the same alarms as the HD-E1 module. Table 80 on page 221 provides a list of the alarms that the system monitors for the DS3/E3 module.

The ALM (alarm status) LED indicates the presence of an active alarm condition of any severity level on any of the three DS3/E3 ports on the module. The LED is lit according to the color codes in Table 87.

Table 87. ALM (Alarm Status) LED for the DS3/E3 Module

LED Color	Description
Green	No alarm is present on any port.
Amber	An alarm is present on one or more ports.
Off	All DS3/E3 ports are disabled.

Downloading Expansion Module Firmware

The system supports the downloading and installation of new firmware in the DS3/E3 module. The procedure is the same as that for the HD-E1 module (see "Downloading Expansion Module Firmware" on page 223).

Chapter 10 **STM-1 Expansion Module**

Chapter contents

Introduction

As an option, the system allows the installation of an STM-1 expansion module for applications that require access to additional STM-1 interface signals. Two types of STM-1 modules are available:

- 2-port G.957 optical STM-1 module
- 2-port G.703 electrical STM-1 module

Figure 143 provides a front view of both types of modules.

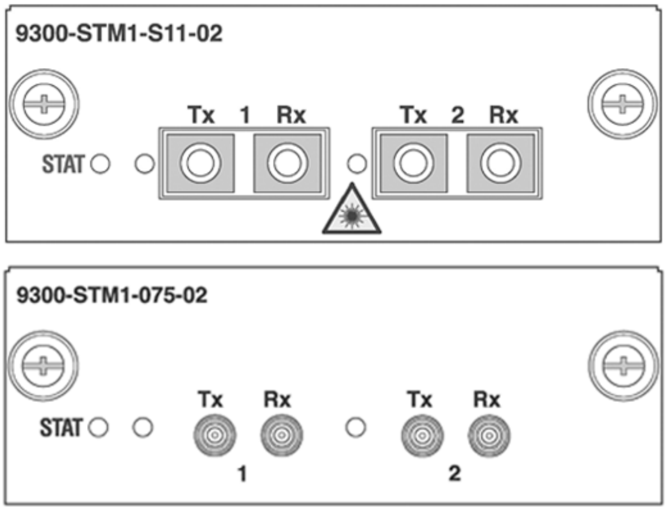


Figure 143. STM-1 Optical and Electrical Interface Modules

The modules weigh approximately 0.2 kg (0.5 lbs) and have the following dimensions: 38 x 101 x 167 mm (height x weight x depth).

Table 88 provides the interconnection parameters for the STM-1 port options.

Table 88. STM-1 Port Interconnection Parameters

Parameter	Electrical STM-1 Ports	Optical STM-1 Ports
Connector	DIN 1.0/2.3	Duplex SC
Termination	75-ohm, unbalanced	–
Line code	CMI	NRZ
Interconnecting cable	Coaxial cable	SMF (single-mode fiber)
Reach	450 feet (137 meters)	S-1.1 L-1.1 L-1.2

The STM-1 ports on the module work in the same way as described in 3, “STM-1 Interface” on page 72 for the STM-1 ports on the base system.

Note The system uses the following naming convention for STM-1 interfaces: ST:slot/port. If the system is equipped with an STM-1 expansion module in slot 2, the two ports are designated as ST:2/1 and ST:2/2. Likewise, if the module is in slot 3, the two ports are designated as ST:3/1 and ST:3/2.

The system supports a single STM-1 of bandwidth between the module and the central switch matrix on the base system. That is, the module supports up to 3 VC-3, 63 VC-12, or an equivalent mix of VC-3 and VC-12/VC-11 connections to the switch matrix.

Unlike the STM-1 ports on the base system, the payload structure for both STM-1 ports in the module needs to be the same when operating in unprotected mode.

CAUTION To protect your eyes, never look at the transmit LED or laser of the STM-1 optical interface (STM-1o) module through a magnifying device while it is powered on. Never look directly at a fiber port on the module or at the ends of fiber cable when they are powered on.

Installing the STM-1 Module

The STM-1 module supports hot swapping. You can insert the module into or remove it from any available expansion slot of the chassis while the system is powered on and carrying traffic. This process does not result in the loss or disruption of existing traffic on the system.

To install the STM-1 module, see Figure 144 on page 239 and follow these steps:

Note Although not required, you may power down the system before starting the module insertion procedure.

1. Remove the front plate cover for the slot in which you wish to install the module. Turn each mounting screw in a counterclockwise direction until the cover is fully released from the chassis.
2. Remove the STM-1 module from the ESD bag and place it on a flat, clean, and dry surface (use a grounded antistatic mat, if possible).

Note Set the ESD bag aside for reuse in case you need it to replace and return the module in the future.

3. Align the module with the card guides inside the slot and slide the module slowly into the slot.

CAUTION Be careful to maintain the alignment along the card cage guide rail axis as you insert the module. Do not rotate or pull the module up or down during the insertion procedure, or you may risk breaking the module.

4. Push the front plate (gently applying force on each side of the plate at the same height as the guide rail) until the module is securely snapped in place. The front plate should be flush with the front panel of the OS-10 system.

5. Secure the module to the chassis by turning the two mounting screws on the front panel of the module in a clockwise direction.

The STAT LED of the STM-1 module becomes a solid amber light for about 10 seconds after the system detects the module. At this point, use the OnSight Device Manager to set the **Administrative Type** for the slot in which the module resides to **2-port STM-1o expansion module** (or **2-port STM-1 e expansion module**). The STAT LED of the module becomes a solid green light when the **Administrative Statu**s of the module is enabled and the **Operational Status** is in service (**IS**).

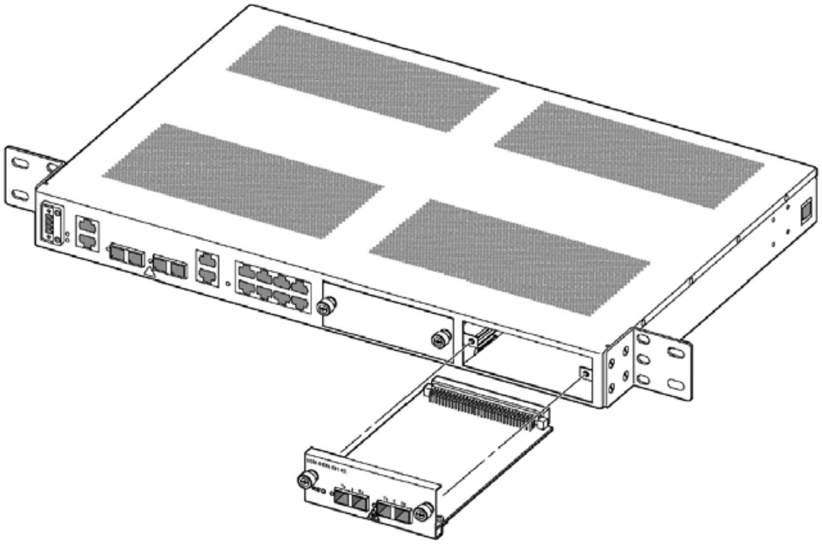


Figure 144. Installing the STM-1 Optical Interface Module

Provisioning the STM-1 Module

To provision the STM-1 optical interface (STM-1o) module, see Figure 152 and follow these steps:

1. Select the **CHASSIS** folder from the navigation menu.
2. From the expanded **CHASSIS** folder, select **Slots.**
3. On the **Slots** page, check that the Status for the slot in which the module resides is **Full**.

> **Note** On the **Slots** page, the **Status** indicates the presence of a module in the expansion slots. When a module is physically present and properly inserted in slot 2 or 3, the table entry shows **Full** for that slot. Otherwise, the table entry shows **Empty**.

4. Check that the **Operational Type** for the slot shows: **2-port STM-1o expansion module** for the STM-1 optical module.

> **Note** The **Operational Type** indicates the type of module in the slot. The table entry shows **2-port STM-1o expansion module** when the system has software access and control for the STM-1 module. Otherwise, the entry shows **Unknown** even when the module is physically present in the slot.

Note When the Operational Type is Unknown and the module is securely installed in the chassis, the module may need replacement. Consult your nearest support center or systems engineer servicing the system for technical support.

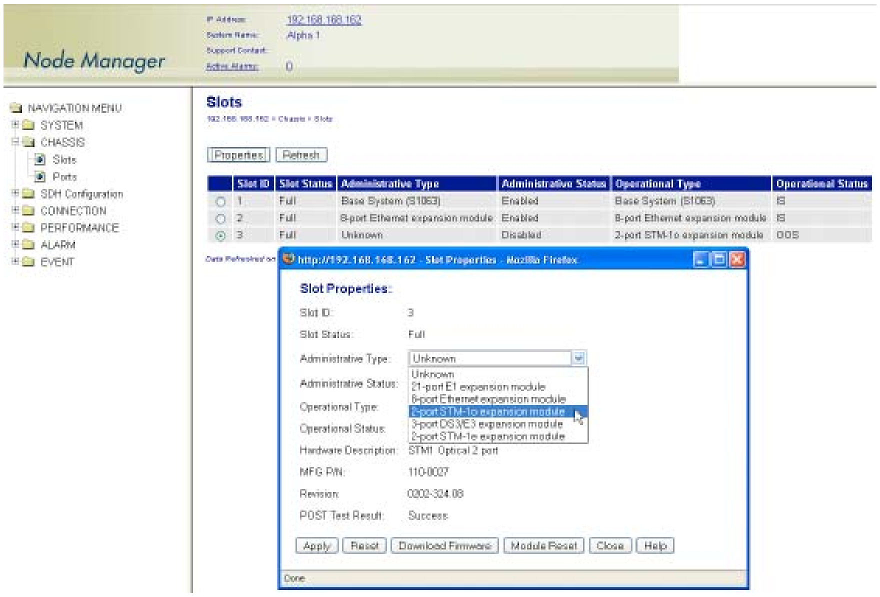
5. Select the **Slot ID** for the slot in which the module resides, and click on **Properties.**
6. In the **Slot Properties** window, set the **Administrative Type** to **2-port STM-1o expansion module** using the scroll-down button.
7. Set the **Administrative Status** to **Enabled**.
8. Click on **Apply** for the settings to take effect.

Note You can also use the **Slot Properties** window to check the inventory for the module, including the hardware description, manufacturing part number (MFG P/N), and revision. You can also use the **Slot Properties** window to verify that the module completed the POST.

Note Click on **Close** to close the window and finish this task.

At this point, the module is now ready for the provisioning of services using the OnSight Device Manager or NMS.

To provision the STM-1 electrical interface (STM-1e) module, follow the preceeding steps but use **2-port STM-1e expansion module** in Step 4 and Step 6.



IP Address: 192.168.168.162
System Name: Alpha 1
Support Contact:
Active Alarms: 0

Slots

192.168.168.162 > Chassis > Slots

	Slot ID	Slot Status	Administrative Type	Administrative Status	Operational Type	Operational Status
○	1	Full	Base System (S1063)	Enabled	Base System (S1063)	IS
○	2	Full	8-port Ethernet expansion module	Enabled	8-port Ethernet expansion module	IS
●	3	Full	Unknown	Disabled	2-port STM-1o expansion module	OOS

Data Refreshed on

http://192.168.168.162 - Slot Properties - Mozilla Firefox

Slot Properties:

Slot ID: 3
Slot Status: Full
Administrative Type: Unknown
- Unknown
- 21-port E1 expansion module
- 8-port Ethernet expansion module
- 2-port STM-1o expansion module
- 3-port DS3/E3 expansion module
- 2-port STM-1e expansion module

Administrative Status:
Operational Type:
Operational Status:
Hardware Description: STM1 Optical 2 port
MFG P/N: 110-0027
Revision: 0202-324.08
POST Test Result: Success

Figure 145. Provisioning the STM-1 Optical Interface Module

The system displays all STM-1 ports in slot 2 and slot 3 when the **Administrative Type** for those slots is set to **Enabled.** The module need not be physically present in the slot for the system to display the ports on the **Ports** page.

You can preconfigure connections to the STM-1 ports before the module is physically present in the slot.

The system maintains all existing connections to the STM-1 expansion ports in the **Client Port Mappings** and **Cross-Connections** tables even after physical removal of the module from the slot.

CAUTION

Save the system configuration to prevent the loss of the module settings if a system reboot occurs.

Module Alarms

The STM-1 module supports the same alarms as the HD-E1 module. Table 80 on page 221 provides a list of the alarms that the system monitors for the STM-1 module.

The ALM (alarm status) LED for each STM-1 port indicates the presence of an active alarm condition of any severity level. The LED is lit according to the color codes in Table 89.

Table 89. ALM (Alarm Status) LED for STM-1 Ports

LED Color	Description
Green	No alarm is present on the port.
Amber	An alarm is present on the port.
Off	The STM-1 port is disabled.

Synchronization

To configure the system to use STM-1 ports 1 and 2 from an STM-1 module as the primary and secondary references for synchronization using line timing, follow these steps:

1. Select the **SYSTEM** folder from the navigation menu.
2. From the expanded **SYSTEM** folder, select **Timing & Sync**.
3. On the **Timing & Synchronization** page, select **Auto: STM-1 Expansion port 2/1, port 2/2** using the **Timing Mode – Primary/Secondary Source** scroll-down button.
4. Click on **Apply** for the changes to take effect.

Note The system does not allow the change of the timing mode directly from one primary-and secondary-timing-source pair to another. You must first change the timing mode to Internal and then to **Auto: STM-1 Expansion port 2/1, port 2/2**. The scroll-down list includes **Auto: STM-1 Expansion port 3/1, port 3/2**, if the system is equipped with an STM-1 module in slot 3.

Downloading Expansion Module Firmware

The system supports the downloading and installation of new firmware in the STM-1 module. The procedure is the same as that for the HD-E1 module (see “Downloading Expansion Module Firmware” on page 223).

Chapter 11 Contacting Patton for assistance

Chapter contents

Introduction

This chapter contains the following information:

- "Contact information"—describes how to contact Patton technical support for assistance.
- "Warranty Service and Returned Merchandise Authorizations (RMAs)"—contains information about the RAS warranty and obtaining a return merchandise authorization (RMA).

Contact information

Patton Electronics offers a wide array of free technical services. If you have questions about any of our other products we recommend you begin your search for answers by using our technical knowledge base. Here, we have gathered together many of the more commonly asked questions and compiled them into a searchable database to help you quickly solve your problems.

- Online support—available at **www.patton.com**.
- E-mail support—e-mail sent to **support@patton.com** will be answered within 1 business day
- Telephone support—standard telephone support is available Monday through Friday, from 8:00 A.M. to 5:00 P.M. EST (8:00 to 17:00 UTC-5), Monday through Friday by calling **+1 (301) 975-1007**

Warranty Service and Returned Merchandise Authorizations (RMAs)

Patton Electronics is an ISO-9001 certified manufacturer and our products are carefully tested before shipment. All of our products are backed by a comprehensive warranty program.

Note If you purchased your equipment from a Patton Electronics reseller, ask your reseller how you should proceed with warranty service. It is often more convenient for you to work with your local reseller to obtain a replacement. Patton services our products no matter how you acquired them.

Warranty coverage

Our products are under warranty to be free from defects, and we will, at our option, repair or replace the product should it fail within one year from the first date of shipment. Our warranty is limited to defects in workmanship or materials, and does not cover customer damage, lightning or power surge damage, abuse, or unauthorized modification.

Out-of-warranty service

Patton services what we sell, no matter how you acquired it, including malfunctioning products that are no longer under warranty. Our products have a flat fee for repairs. Units damaged by lightning or elephants may require replacement.

Returns for credit

Customer satisfaction is important to us, therefore any product may be returned with authorization within 30 days from the shipment date for a full credit of the purchase price. If you have ordered the wrong equipment or you are dissatisfied in any way, please contact us to request an RMA number to accept your return. Patton is not responsible for equipment returned without a Return Authorization.

Return for credit policy

- Less than 30 days: No Charge. Your credit will be issued upon receipt and inspection of the equipment.
- 30 to 120 days: We will add a 20% restocking charge (crediting your account with 80% of the purchase price).
- Over 120 days: Products will be accepted for repairs only.

RMA numbers

RMA numbers are required for all product returns. You can obtain an RMA by doing one of the following:

- Completing a request on the RMA Request page in the *Support* section at **www.patton.com**
- By calling **+1 (301) 975-1000** and speaking to a Technical Support Engineer
- By sending an e-mail to **returns@patton.com**

All returned units must have the RMA number clearly visible on the outside of the shipping container. Please use the original packing material that the device came in or pack the unit securely to avoid damage during shipping.

Shipping instructions

The RMA number should be clearly visible on the address label. Our shipping address is as follows:

Patton Electronics Company
RMA#: xxxx
7622 Rickenbacker Dr.
Gaithersburg, MD 20879-4773 USA

Patton will ship the equipment back to you in the same manner you ship it to us. Patton will pay the return shipping costs.

Appendix A **Terms and Acronyms**

Chapter contents

Abbreviations

Abbreviation	Meaning
A	
AIS	Alarm Indication Signal
AMI	Alternate Mark Inversion
AU	Administrative Unit
AUX	Auxiliary (port)
B	
BIP	Bit Interleaved Parity
BBE	Background Block Error
BER	Bit Error Rate
BPV	Bipolar Violation
B3ZS	Bipolar with 3-zero Substitution
B8ZS	Bipolar with 8-zero Substitution
C	
cHEC	core Header Error Check
CLI	Command Line Interface
CSU/DSU	Channel Service Unit/Data Service Unit
C-Tag	Customer-assigned tag (for example, VLAN tag)
D	
DNU	Do Not Use (for synchronization)
E	
E1	European digital signal hierarchy level 1
EB	Errored Block
EDC	Error Detection Code
EIA	Electronics Industries Alliance
EOW	Engineering Orderwire
ES	Errored Second
ETSI	European Telecommunications Standards Institute
EXM	Extension Header Mismatch
EXZ	Excessive Zeros
G	
GFP	Generic Framing Procedure
H	
HDB3	High-Density Bipolar with 3-zero Substitution
HP	High-order Path
HTTP	Hyper Text Transfer Protocol
I	
IP	Internet Protocol

Abbreviation	Meaning
L	
LCAS	Link Capacity Adjustment Scheme
LFD	Loss of Frame Delineation
LOF	Loss of Frame
LOP	Loss of Pointer
LP	Low-order Path
M	
MS	Multiplex Section
N	
NEBS	Network Equipment Building System
NEC	National Electric Code
P	
PBX	Private Branch Exchange
PC	Personal Computer
PDH	Plesiochronous Digital Hierarchy
PJC	Pointer Justification Count
PM	Performance Monitoring
POST	Power-On Self-Test
ppm	parts per million
PRC	Primary Reference Clock
PRI	Primary Rate Interface
PSC	Protection Switching Count
PSD	Protection Switching Duration
R	
RS	Regenerator Section
RSOH	Regenerator Section Overhead
RU	Rack Unit (1.75 inches)
S	
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SEC	Secondary source (also Synchronous Equipment Clock)
SES	Severely Errored Second
SF	Signal Failure
SNMP	Simple Network Management Protocol
SOH	Section Overhead
SSM	Synchronization Status Messaging
SSU	Synchronization Supply Unit
S-Tag	Service provider tag
STM-1	Synchronous Transport Module level 1

Abbreviation	Meaning
T	
TDM	Time Division Multiplexing
TIA	Telecommunications Industry Association
TIM	Trace Identifier Mismatch
TNV	Telecommunications Network Voltage
TP	Termination Point
TU	Tributary Unit
TUG	Tributary Unit Group
U	
UAS	Unavailable Seconds