



General Troubleshooting



Note

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15454. To troubleshoot specific ONS 15454 alarms, see [Chapter 2, "Alarm Troubleshooting."](#) If you cannot find what you are looking for, contact the Cisco Technical Assistance Center (1 800 553-2447).



Note

Release 4.7 is DWDM only. It supports all DWDM, transponder (TXP), and muxponder (MXP) cards but not optical, electrical, fibre storage, or Ethernet cards.

This chapter includes the following sections on network problems:

- [1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks, page 1-2](#)—Describes loopbacks, which you can use to test circuit paths through the network or logically isolate faults.
- [1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks, page 1-5](#)—Explains how to use loopbacks tests described in "[Troubleshooting Non-DWDM Circuit Paths with Loopbacks](#)" to isolate trouble on MXP or TXP circuits.
- [1.3 Troubleshooting DWDM Circuit Paths With G.709 Monitoring, page 1-20](#)—Explains how to use performance monitoring (PM) and threshold crossing alerts (TCA) to locate signal degrades on DWDM circuit paths.



Note

To perform a DWDM network acceptance test, refer to NTP-G16 in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

The remaining sections describe symptoms, problems, and solutions that are categorized according to the following topics:

- [1.4 Using CTC Diagnostics, page 1-28](#)—Explains how to perform card LED tests, download a diagnostic file for Technical Support, and create a diagnostic standby BLSR circuit.
- [1.5 Restoring the Database and Default Settings, page 1-33](#)—Provides procedures for restoring software data and restoring the node to the default setup.

- [1.6 PC Connectivity Troubleshooting, page 1-39](#)—Provides troubleshooting procedures for PC and network connectivity to the ONS 15454.
- [1.7 CTC Operation Troubleshooting, page 1-45](#)—Provides troubleshooting procedures for CTC login or operation problems.
- [1.8 Circuits and Timing, page 1-58](#)—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.
- [1.9 Fiber and Cabling, page 1-63](#)—Provides troubleshooting procedures for fiber and cabling connectivity errors.
- [1.10 Power Supply Problems, page 1-72](#)—Provides troubleshooting procedures for power supply problems.

1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks

Use loopbacks to test newly created SONET circuits before running live traffic or to logically locate the source of a network failure. ONS 15454 muxponder (MXP) and transponder (TXP) cards used in DWDM configurations allow loopbacks. DWDM cards such as OPT-BST, OPT-PRE, OSC-CSM, and optical add/drop multiplexer cards (band add-drop cards and channel add-drop cards) do not allow loopbacks.

To create a loopback on a port, the port must be in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state. The resulting service state is Out-of-Service and Management, Loopback and Maintenance (OOS-MA,LPBK & MT).



Caution

Facility (line) or terminal loopbacks can be service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. Basic directions for these external switching commands exist in [Chapter 2, “Alarm Troubleshooting.”](#)



Note

In Software Release 4.7, loopbacks are not available for DWDM cards. DWDM cards include the OSCM, OSC-CSM, OPT-PRE, OPT-BST, 32MUX-O, 32DMX-O, 32DMX, 4MD-xx.xAD-4B-xx.x, AD-1B-xx.x, AD-4C-xx.x, AD-2C-xx.x, AD-1C-xx.x, and the 32WSS.

1.1.1 Facility Loopbacks

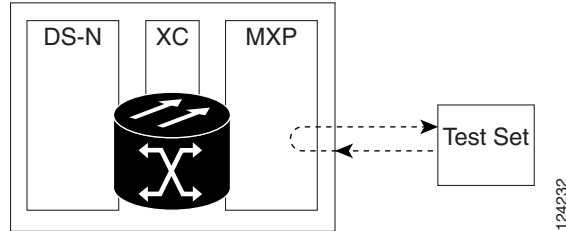
The following sections give general information about facility loopback operations and specific information about ONS 15454 card loopback activity.

1.1.1.1 General Behavior

A facility (line) loopback tests the line interface unit (LIU) of a card, the EIA (electrical interface assembly), and related cabling. After applying a facility loopback on a port, use a test set to run traffic over the loopback. A successful facility loopback isolates the LIU, the EIA, or the cabling plant as the potential cause of a network problem.

To test an MXP card LIU, connect an optical test set to the MXP port and perform a facility (line) loopback. Or use a loopback on a card that is farther along the circuit path. [Figure 1-1](#) shows a facility loopback on an MXP card.

Figure 1-1 Facility (Line) Loopback Path on a Near-End MXP Card



1.1.1.2 ONS 15454 Card Behavior

ONS 15454 port loopbacks either terminate or bridge the loopback signal. ONS 15454 MXP and TXP facility loopbacks are terminated as shown in [Table 1-1](#).

When a port terminates a facility loopback signal, the signal only loops back to the originating port and is not transmitted downstream. When a port bridges a loopback signal, the signal loops back to the originating port and is also transmitted downstream.



Note

In [Table 1-1](#), no AIS signal is injected if the signal is bridged. If the signal is terminated, an applicable AIS is injected downstream for all cards except Ethernet cards.

Table 1-1 ONS 15454 MXP and TXP Facility Loopback Behavior

Card/Port	Facility loopback signal
MXP, MXPP trunk ports	Bridged
MXP, MXPP client ports	Terminated
TXP, TXPP trunk ports	Bridged
TXP, TXPP client ports	Terminated

MXP, TXP, and FC_MR card facility loopbacks can have different service states for the trunk and client ports. With a client-side facility loopback, the client port service state is Out-of-Service and Management, Loopback and Maintenance (OOS-MA,LPBK & MT); however the remaining client and trunk ports can be in any other service state. For cards in a trunk-side facility loopback, the trunk port service state is OOS-MA,LPBK & MT service state and the remaining client and trunk ports can be in any other service state.

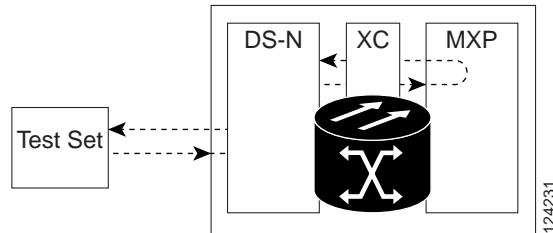
1.1.2 Terminal Loopbacks

The following sections give general information about terminal loopback operations and specific information about ONS 15454 card MXP and TXP loopback activity.

1.1.2.1 General Behavior

A terminal loopback tests a circuit path as it passes through the cross-connect card (XC10G) and loops back from the card with the loopback. [Figure 1-2](#) shows a terminal loopback on an MXP card. The test-set traffic comes into the electrical port and travels through the cross-connect card to the optical card. The terminal loopback on the optical card turns the signal around before it reaches the LIU and sends it back through the cross-connect card to the electrical card. This test verifies that the cross-connect card and terminal circuit paths are valid, but does not test the LIU on the optical card.

Figure 1-2 Terminal Loopback Path on an MXP Card



1.1.2.2 ONS 15454 Card Behavior

ONS 15454 terminal port loopbacks can either terminate or bridge the signal. In ONS 15454 MXP and TXP cards, terminal loopbacks are terminated as shown in [Table 1-2](#). During terminal loopbacks, some ONS 15454 cards bridge the loopback signal while others terminate it.

If a port terminates a terminal loopback signal, the signal only loops back to the originating port and is not transmitted downstream. If the port bridges a loopback signal, the signal loops back to the originating port and is also transmitted downstream.

MXP and TXP card terminal loopback bridging and terminating behaviors are listed in [Table 1-2](#).



Note

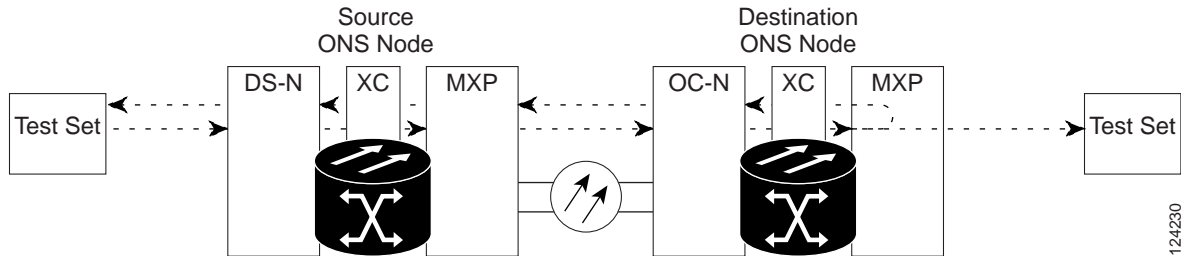
In [Table 1-2](#), no AIS signal is injected if the signal is bridged. If the signal is terminated, an applicable AIS is injected downstream for all cards except Ethernet cards.

Table 1-2 ONS 15454 MXP Card Terminal Loopback Behavior

Card/Port	Terminal loopback signal
MXP, MXPP trunk ports	Bridged
MXP, MXPP client ports	Terminated
TXP, TXPP trunk ports	Bridged
TXP, TXPP client ports	Terminated

A bridged terminal loopback signal is shown in [Figure 1-3](#).

Figure 1-3 Terminal Loopback on an MXP Card with Bridged Signal



TXP and MXP card trunk and client ports have different service state behaviors and requirements from other ONS 15454 cards. The cards can simultaneously maintain different service states.

- For TXP and TXPP cards with a client-side terminal loopback, the client port is in the OOS-MA,LPBK & MT service state and trunk port must be in IS-NR service state.
- For MXP and MXPP cards with a client-side terminal loopback the client port is in the OOS-MA,LPBK & MT service state and the remaining client and trunk ports can be in any service state.
- In MXP or TXP trunk-side terminal loopbacks, the trunk port is in the OOS-MA,LPBK & MT service state and the client ports must be in IS-NR for complete loopback functionality. A terminal loopback affects all client ports because it is performed on the aggregate signal.

The loopback itself is listed in the Conditions window. For example, the window would list the LPBKTERMINAL condition or LPBKFACILITY condition for a tested port. (The Alarms window will show AS-MT, which indicates that all alarms are suppressed on the port during loopback testing.)

In addition to the Conditions window listing, the following behaviors occur:

- If an electrical or optical port is in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state, it injects an AIS signal upstream and downstream.
- When an electrical or optical port is placed in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state before loopback testing, the port clears the AIS signal upstream and downstream unless there is a service-affecting defect that would also cause an AIS signal to be injected. For more information about placing ports into alternate states for testing, refer to the *Cisco ONS 15454 Procedure Guide*.

1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks

Facility (line) loopbacks and terminal (inward) loopbacks are often used together to test the circuit path through the network or to logically isolate a fault. Performing a loopback test at each point along the circuit path systematically isolates possible points of failure. MXP and TXP loopback testing does not require circuit creation (unlike optical, electrical, or Ethernet cards used in SONET and SDH ONS platforms). MXP and TXP client ports are statically mapped to the trunk ports so no signal needs to traverse the cross-connect card (in a circuit) to test the loopback.

The example in this section tests a circuit on a three-node BLSR. Using a series of facility (line) loopbacks and terminal (inward) loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them.

1.2.1 Perform a Facility (Line) Loopback on a Source-Node MXP or TXP Port

The logical progression contains seven network test procedures:



Note

In Software R4.7, loopbacks are not available for DWDM cards. DWDM cards include the OSCM, OSC-CSM, OPT-PRE, OPT-BST, 32MUX-O, 32DMX-O, 32DMX, 4MD-xx.xAD-4B-xx.x, AD-1B-xx.x, AD-4C-xx.x, AD-2C-xx.x, AD-1C-xx.x, and the 32WSS.



Note

MXP and TXP card client ports do not appear in the Maintenance > Loopback tab unless they have been provisioned. Do this in the card view Provisioning > Pluggable Port Modules tab. For information about provisioning client ports, refer to the *Cisco ONS 15454 Procedure Guide*.



Note

The test sequence for your circuits will differ according to the type of circuit and network topology.

1. A facility (line) loopback on the source-node MXP or TXP port
2. A terminal (inward) loopback on the source-node MXP or TXP port
3. A facility (line) loopback on the intermediate-node MXP or TXP port
4. A terminal (inward) loopback on the intermediate-node MXP or TXP port
5. A facility (line) loopback on the destination-node MXP or TXP port
6. A terminal (inward) loopback on the destination-node MXP or TXP port



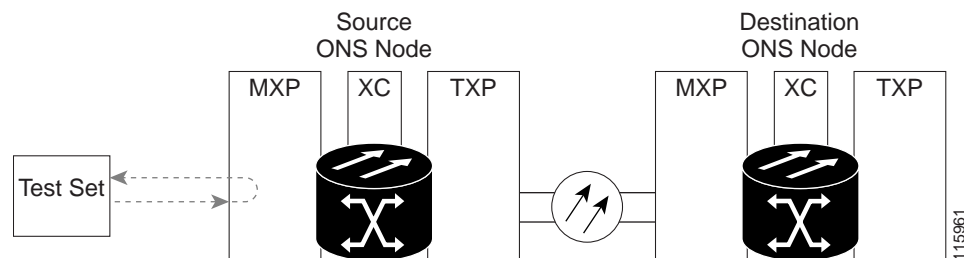
Note

Facility and terminal loopback tests require on-site personnel.

1.2.1 Perform a Facility (Line) Loopback on a Source-Node MXP or TXP Port

The facility (line) loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the loopback is performed on the source-node muxponder or transponder port. Completing a successful facility (line) loopback on this port isolates the port as a possible failure point. [Figure 1-4](#) shows an example of a facility loopback on a circuit source port.

Figure 1-4 Facility (Line) Loopback on a Circuit Source MXP or TXP Port



Caution

Performing a loopback on an in-service circuit is service-affecting.

Complete the [“Create the Facility \(Line\) Loopback on the Source-Node MXP or TXP Port”](#) procedure on page 1-7.

Create the Facility (Line) Loopback on the Source-Node MXP or TXP Port

Step 1 Connect an optical test set to the port you are testing.



Note Refer to the manufacturer’s instructions for detailed information about connection and setup of the optical test set.

Use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. The Tx and Rx terminals connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 In CTC node view, double-click the card to display the card view.

Step 4 Click the **Maintenance > Loopback** tab.

Step 5 Choose **OOS,MT** from the Admin State column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

Step 6 Choose **Facility (Line)** from the Loopback Type column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

Step 7 Click **Apply**.

Step 8 Click **Yes** in the confirmation dialog box.



Note It is normal for a [“LPBKFACILITY \(OCN\)”](#) condition on page 2-159, or a [“LPBKFACILITY \(G1000\)”](#) condition on page 2-157 to appear during loopback setup. The condition clears when you remove the loopback.

Step 9 Complete the [“Test and Clear the MXP or TXP Facility \(Line\) Loopback Circuit”](#) procedure on page 1-7.

Test and Clear the MXP or TXP Facility (Line) Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility (line) loopback:

- a. Click the **Maintenance > Loopback** tab.
- b. Choose **None** from the Loopback Type column for the port being tested.
- c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) from the Admin State column for the port being tested.
- d. Click **Apply**.
- e. Click **Yes** in the confirmation dialog box.

- Step 4** Complete the [“Create the Terminal \(Inward\) Loopback on a Source-Node MXP or TXP Port” procedure on page 1-9](#). If the test set indicates a faulty circuit, the problem might be a faulty card.
- Step 5** Complete the [“Test the MXP or TXP Card” procedure on page 1-8](#).
-

Test the MXP or TXP Card

- Step 1** Complete the [“Physically Replace a Traffic Card” procedure on page 2-252](#) for the suspected bad card and replace it with a known-good one.



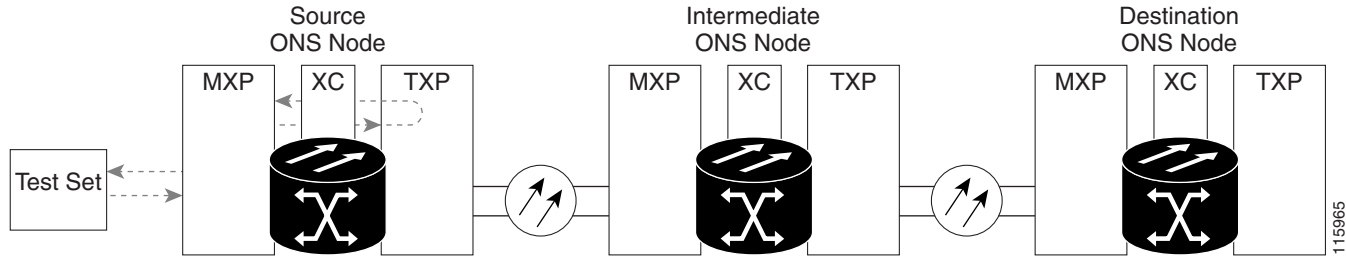
Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the [“Protection Switching, Lock Initiation, and Clearing” section on page 2-242](#). For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

- Step 2** Resend test traffic on the loopback circuit with a known-good card installed.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).
- Step 4** Complete the [“Physically Replace a Traffic Card” procedure on page 2-252](#) for the faulty card.
- Step 5** Clear the facility (line) loopback:
- a. Click the **Maintenance > Loopback** tab.
 - b. Choose **None** from the Loopback Type column for the port being tested.
 - c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) from the Admin State column for the port being tested.
 - d. Click **Apply**.
 - e. Click **Yes** in the confirmation dialog box.
- Step 6** Complete the [“Perform a Terminal \(Inward\) Loopback on a Source-Node MXP or TXP Port” procedure on page 1-8](#).
-

1.2.2 Perform a Terminal (Inward) Loopback on a Source-Node MXP or TXP Port

The terminal (inward) loopback test is performed on the node source MXP, TXP, or FC_MR port. For the circuit in this example, it is the source-node MXP port. You first create a bidirectional circuit that starts on the node destination MXP or TXP port and loops back on the node source port. You then proceed with the terminal loopback test. Completing a successful terminal loopback to a node source port verifies that the circuit is good to the source port. [Figure 1-5](#) shows an example of a terminal loopback on a source port.

Figure 1-5 Terminal (Inward) Loopback on a Source-Node MXP or TXP Port



Caution

Performing a loopback on an in-service circuit is service-affecting.

Complete the [“Create the Terminal \(Inward\) Loopback on a Source-Node MXP or TXP Port” procedure on page 1-9.](#)

Create the Terminal (Inward) Loopback on a Source-Node MXP or TXP Port

Step 1 Connect an optical test set to the port you are testing:



Note

Refer to the manufacturer’s instructions for detailed information about connection and setup of the optical test set.

- a. If you just completed the [“Perform a Facility \(Line\) Loopback on a Source-Node MXP or TXP Port” procedure on page 1-6](#), leave the optical test set hooked up to the source-node MXP or TXP port.
- b. If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 In node view, double-click the card that requires the loopback, such as the destination OC-N card in the source node.

Step 4 Click the **Maintenance > Loopback** tab.

Step 5 Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

Step 6 Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

Step 7 Click **Apply**.

Step 8 Click **Yes** in the confirmation dialog box.

Step 9 Complete the [“Test and Clear the MXP or TXP Port Terminal Loopback Circuit” procedure on page 1-10.](#)

Test and Clear the MXP or TXP Port Terminal Loopback Circuit

-
- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Clear the terminal loopback state on the port:
- Double-click the card in the source node with the terminal loopback.
 - Click the **Maintenance > Loopback** tab.
 - Select **None** from the Loopback Type column for the port being tested.
 - Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.
 - Click **Apply**.
 - Click **Yes** in the confirmation dialog box.
- Step 4** Complete the [“Create a Facility \(Line\) Loopback on an Intermediate-Node MXP or TXP Port” procedure on page 1-11](#). If the test set indicates a faulty circuit, the problem might be a faulty card.
- Step 5** Complete the [“Test the MXP or TXP Card” procedure on page 1-10](#).
-

Test the MXP or TXP Card

-
- Step 1** Complete the [“Physically Replace a Traffic Card” procedure on page 2-252](#) for the suspected bad card and replace it with a known-good one.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the [“Protection Switching, Lock Initiation, and Clearing” section on page 2-242](#). For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

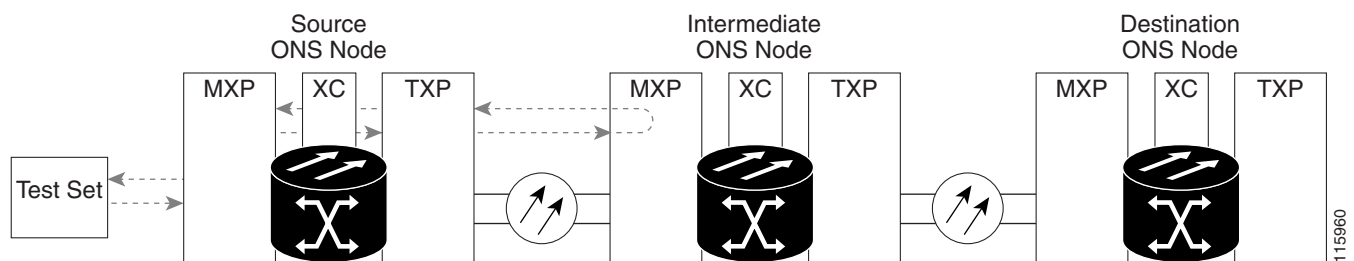
- Step 2** Resend test traffic on the loopback circuit with a known-good card.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).
- Step 4** Complete the [“Physically Replace a Traffic Card” procedure on page 2-252](#) for the defective card.
- Step 5** Clear the terminal loopback on the port before testing the next segment of the network circuit path:
- Double-click the card in the source node with the terminal loopback.
 - Click the **Maintenance > Loopback** tab.
 - Select **None** from the Loopback Type column for the port being tested.
 - Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.
 - Click **Apply**.
 - Click **Yes** in the confirmation dialog box.

- Step 6** Complete the “[Create a Facility \(Line\) Loopback on an Intermediate-Node MXP or TXP Port](#)” procedure on page 1-11.

1.2.3 Create a Facility (Line) Loopback on an Intermediate-Node MXP or TXP Port

Performing the facility (line) loopback test on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in [Figure 1-6](#), the test is being performed on an intermediate MXP or TXP port.

Figure 1-6 Facility (Line) Loopback on an Intermediate-Node MXP or TXP Port



Caution Performing a loopback on an in-service circuit is service-affecting.

Complete the “[Create a Facility \(Line\) Loopback on an Intermediate-Node MXP or TXP Port](#)” procedure on page 1-11.

Create a Facility (Line) Loopback on an Intermediate-Node MXP or TXP Port

- Step 1** Connect an optical test set to the port you are testing:



Note Refer to the manufacturer’s instructions for detailed information about connection and setup of the optical test set.

- a. If you just completed the “[Perform a Terminal \(Inward\) Loopback on a Source-Node MXP or TXP Port](#)” procedure on page 1-8, leave the optical test set hooked up to the source-node port.
- b. If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

- Step 2** Adjust the test set accordingly.

- Step 3** In node view, double-click the intermediate-node card that requires the loopback.

- Step 4** Click the **Maintenance > Loopback** tab.

- Step 5** Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

- Step 6 Select **Facility (Line)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
 - Step 7 Click **Apply**.
 - Step 8 Click **Yes** in the confirmation dialog box.
 - Step 9 Complete the [“Test and Clear the MXP or TXP Port Facility \(Line\) Loopback Circuit” procedure on page 1-12](#).
-

Test and Clear the MXP or TXP Port Facility (Line) Loopback Circuit

- Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.
 - Step 2 Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
 - Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility (line) loopback. Clear the facility loopback from the port:
 - a. Click the **Maintenance > Loopback** tab.
 - b. Choose **None** from the Loopback Type column for the port being tested.
 - c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) from the Admin State column for the port being tested.
 - d. Click **Apply**.
 - e. Click **Yes** in the confirmation dialog box.
 - Step 4 Complete the [“Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports” procedure on page 1-14](#). If the test set indicates a faulty circuit, the problem might be a faulty MXP or TXP card.
 - Step 5 Complete the [“Test the MXP or TXP Card” procedure on page 1-12](#).
-

Test the MXP or TXP Card

- Step 1 Complete the [“Physically Replace a Traffic Card” procedure on page 2-252](#) for the suspected bad card and replace it with a known-good one.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the [“Protection Switching, Lock Initiation, and Clearing” section on page 2-242](#). For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

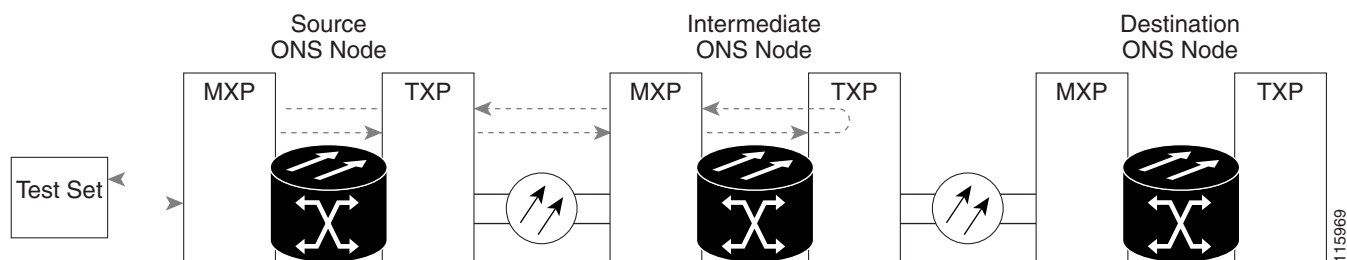
- Step 2 Resend test traffic on the loopback circuit with a known-good card installed.
- Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).
- Step 4 Complete the [“Physically Replace a Traffic Card” procedure on page 2-252](#) for the faulty card.

- Step 5** Clear the facility (line) loopback from the port:
- Click the **Maintenance > Loopback** tab.
 - Choose **None** from the Loopback Type column for the port being tested.
 - Choose the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) from the Admin State column for the port being tested.
 - Click **Apply**.
 - Click **Yes** in the confirmation dialog box.
- Step 6** Complete the [“Create a Terminal \(Inward\) Loopback on Intermediate-Node MXP or TXP Ports” procedure on page 1-13.](#)

1.2.4 Create a Terminal (Inward) Loopback on Intermediate-Node MXP or TXP Ports

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in [Figure 1-7](#), the terminal loopback is performed on an intermediate MXP or TXP port in the circuit. You first create a bidirectional circuit that originates on the source-node MXP or TXP port and loops back on the intermediate-node port. You then proceed with the terminal loopback test. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

Figure 1-7 Terminal Loopback on an Intermediate-Node MXP or TXP Port



Caution Performing a loopback on an in-service circuit is service-affecting.

Complete the [“Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports” procedure on page 1-14.](#)

Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports

Step 1 Connect an optical test set to the port you are testing:



Note Refer to the manufacturer's instructions for detailed information about connection and setup of the optical test set.

- a. If you just completed the [“Create a Facility \(Line\) Loopback on an Intermediate-Node MXP or TXP Port”](#) section on page 1-11, leave the optical test set hooked up to the source-node port.
- b. If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Create the terminal loopback on the destination port being tested:

- a. Go to the node view of the intermediate node:
 - Choose **View > Go To Other Node** from the menu bar.
 - Choose the node from the pull-down menu in the Select Node dialog box and click **OK**.
- b. In node view, double-click the card that requires the loopback.
- c. Click the **Maintenance > Loopback** tab.
- d. Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.
- e. Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
- f. Click **Apply**.
- g. Click **Yes** in the confirmation dialog box.

Step 4 Complete the [“Test and Clear the MXP or TXP Terminal Loopback Circuit”](#) procedure on page 1-14.

Test and Clear the MXP or TXP Terminal Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Clear the terminal loopback from the port:

- a. Double-click the intermediate-node card with the terminal loopback to display the card view.
- b. Click the **Maintenance > Loopback** tab.
- c. Select **None** from the Loopback Type column for the port being tested.
- d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.
- e. Click **Apply**.

- f. Click **Yes** in the confirmation dialog box.
 - Step 4 Complete the “[Create the Facility \(Line\) Loopback on a Destination-Node MXP or TXP Port](#)” procedure on page 1-16. If the test set indicates a faulty circuit, the problem might be a faulty card.
 - Step 5 Complete the “[Test the MXP or TXP Card](#)” procedure on page 1-15.
-

Test the MXP or TXP Card

- Step 1 Complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-252 for the suspected bad card and replace it with a known-good one.



Caution

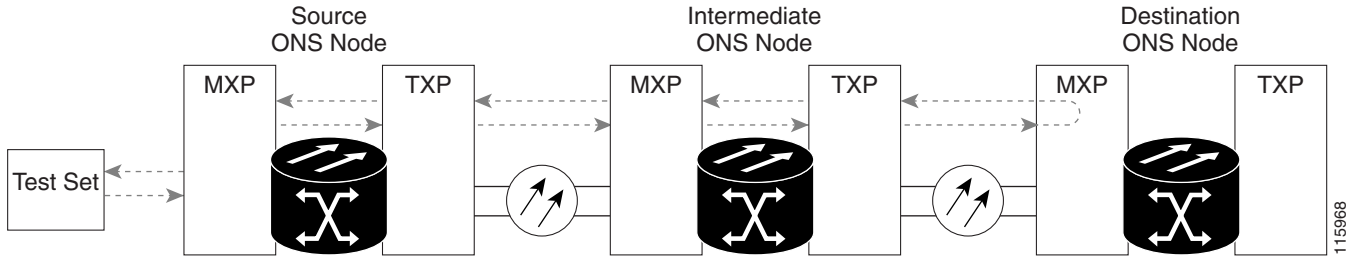
Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the “[Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

- Step 2 Resend test traffic on the loopback circuit with a known-good card.
 - Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).
 - Step 4 Complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-252 for the defective card.
 - Step 5 Clear the terminal loopback on the port:
 - a. Double-click the source-node card with the terminal loopback.
 - b. Click the **Maintenance > Loopback** tab.
 - c. Select **None** from the Loopback Type column for the port being tested.
 - d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.
 - e. Click **Apply**.
 - f. Click **Yes** in the confirmation dialog box.
 - Step 6 Complete the “[Perform a Facility \(Line\) Loopback on a Destination-Node MXP or TXP Port](#)” procedure on page 1-15.
-

1.2.5 Perform a Facility (Line) Loopback on a Destination-Node MXP or TXP Port

You perform a facility (line) loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in [Figure 1-8](#) shows a facility loopback being performed on an MXP or TXP port.

Figure 1-8 Facility (Line) Loopback on a Destination-Node MXP or TXP Port

**Caution**

Performing a loopback on an in-service circuit is service-affecting.

Complete the [“Create the Facility \(Line\) Loopback on a Destination-Node MXP or TXP Port” procedure on page 1-16](#).

Create the Facility (Line) Loopback on a Destination-Node MXP or TXP Port

Step 1 Connect an optical test set to the port you are testing:

**Note**

Refer to the manufacturer’s instructions for detailed information about connection and setup of the optical test set.

- a. If you just completed the [“Create the Terminal \(Inward\) Loopback on a Source-Node MXP or TXP Port” procedure on page 1-9](#), leave the optical test set hooked up to the source-node port.
- b. If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Create the facility (line) loopback on the destination port being tested:

- a. Go to the node view of the destination node:
 - Choose **View > Go To Other Node** from the menu bar.
 - Choose the node from the pull-down menu in the Select Node dialog box and click **OK**.
- b. In node view, double-click the card that requires the loopback.
- c. Click the **Maintenance > Loopback** tab.
- d. Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.
- e. Select **Facility (Line)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
- f. Click **Apply**.
- g. Click **Yes** in the confirmation dialog box.

- Step 4 Complete the [“Test and Clear the MXP or TXP Facility \(Line\) Loopback Circuit” procedure on page 1-17](#).
-

Test and Clear the MXP or TXP Facility (Line) Loopback Circuit

- Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2 Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility (line) loopback from the port:
- Click the **Maintenance > Loopback** tab.
 - Choose **None** from the Loopback Type column for the port being tested.
 - Choose the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) from the Admin State column for the port being tested.
 - Click **Apply**.
 - Click **Yes** in the confirmation dialog box.
- Step 4 Complete the [“Create the Terminal Loopback on a Destination-Node MXP or TXP Port” procedure on page 1-18](#). If the test set indicates a faulty circuit, the problem might be a faulty MXP or TXP card.
- Step 5 Complete the [“Test the MXP or TXP Card” procedure on page 1-17](#).
-

Test the MXP or TXP Card

- Step 1 Complete the [“Physically Replace a Traffic Card” procedure on page 2-252](#) for the suspected bad card and replace it with a known-good one.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the [“Protection Switching, Lock Initiation, and Clearing” section on page 2-242](#). For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

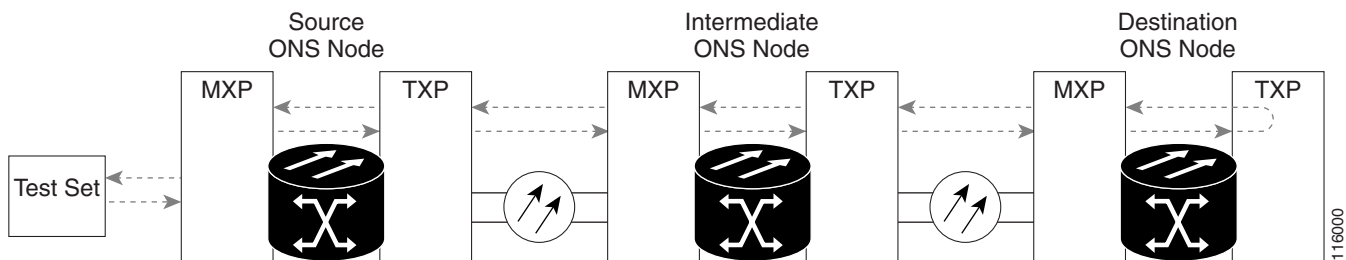
- Step 2 Resend test traffic on the loopback circuit with a known-good card installed.
- Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).
- Step 4 Complete the [“Physically Replace a Traffic Card” procedure on page 2-252](#) for the faulty card.
- Step 5 Clear the facility (line) loopback on the port:
- Click the **Maintenance > Loopback** tab.
 - Choose **None** from the Loopback Type column for the port being tested.
 - Choose the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) from the Admin State column for the port being tested.

- d. Click **Apply**.
 - e. Click **Yes** in the confirmation dialog box.
- Step 6** Complete the “[Perform a Terminal Loopback on a Destination-Node MXP or TXP Port](#)” procedure on page 1-18.

1.2.6 Perform a Terminal Loopback on a Destination-Node MXP or TXP Port

The terminal loopback at the destination-node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in [Figure 1-9](#) shows a terminal loopback on an intermediate-node destination MXP or TXP port.

Figure 1-9 Terminal Loopback on a Destination-Node MXP or TXP port



Caution Performing a loopback on an in-service circuit is service-affecting.

Complete the “[Create the Terminal Loopback on a Destination-Node MXP or TXP Port](#)” procedure on page 1-18.

Create the Terminal Loopback on a Destination-Node MXP or TXP Port

- Step 1** Connect an optical test set to the port you are testing:



Note Refer to the manufacturer’s instructions for detailed information about connection and setup of the optical test set.

- a. If you just completed the “[Perform a Facility \(Line\) Loopback on a Destination-Node MXP or TXP Port](#)” procedure on page 1-15, leave the optical test set hooked up to the source port.
 - b. If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.
- Step 2** Adjust the test set accordingly.
- Step 3** Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.



Note It is normal for the “[LPBKTERMINAL \(OCN\)](#)” condition on page 2-163 to appear during a loopback setup. The condition clears when you remove the loopback.

- Step 4** Create the terminal loopback on the destination port being tested:
- a. Go to the node view of the destination node:
 - Choose **View > Go To Other Node** from the menu bar.
 - Choose the node from the pull-down menu in the Select Node dialog box and click **OK**.
 - b. In node view, double-click the card that requires the loopback.
 - c. Click the **Maintenance > Loopback** tab.
 - d. Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.
 - e. Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
 - f. Click **Apply**.
 - g. Click **Yes** in the confirmation dialog box.
- Step 5** Complete the “[Test and Clear the MXP or TXP Terminal Loopback Circuit](#)” procedure on page 1-19.
-

Test and Clear the MXP or TXP Terminal Loopback Circuit

-
- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Clear the terminal loopback from the port:
- a. Double-click the intermediate-node card with the terminal loopback.
 - b. Click the **Maintenance > Loopback** tab.
 - c. Select **None** from the Loopback Type column for the port being tested.
 - d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.
 - e. Click **Apply**.
 - f. Click **Yes** in the confirmation dialog box.
- Step 4** If the test set indicates a faulty circuit, the problem might be a faulty card.
- Step 5** Complete the “[Test the MXP or TXP Card](#)” procedure on page 1-20.
-

Test the MXP or TXP Card

- Step 1** Complete the [“Physically Replace a Traffic Card” procedure on page 2-252](#) for the suspected bad card and replace it with a known-good card.



Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the [“Protection Switching, Lock Initiation, and Clearing” section on page 2-242](#). For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

- Step 2** Resend test traffic on the loopback circuit with a known-good card.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).
- Step 4** Complete the [“Physically Replace a Traffic Card” procedure on page 2-252](#) for the defective card.
- Step 5** Clear the terminal loopback on the port:
- Double-click the source-node card with the terminal loopback.
 - Click the **Maintenance > Loopback** tab.
 - Select **None** from the Loopback Type column for the port being tested.
 - Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.
 - Click **Apply**.
 - Click **Yes** in the confirmation dialog box.

The entire circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

1.3 Troubleshooting DWDM Circuit Paths With G.709 Monitoring

This section provides an overview of the optical transport network (OTN) specified in ITU-T G.709 Network Node Interface for the Optical Transport Network, and provides troubleshooting procedures for DWDM circuit paths in the G.709 OTN using performance monitoring and threshold crossing alerts (TCAs).

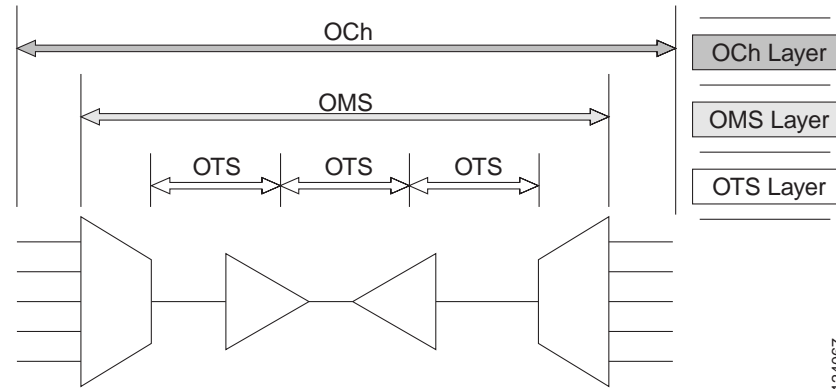
1.3.1 G.709 Monitoring in Optical Transport Networks

Recommendation G.709 is part of a suite of recommendations covering the full functionality of an OTN. G.709 takes single-wavelength SONET technology a step further by enabling transparent optical wavelength-based networks. It adds extra overhead to existing SONET, Ethernet, or ATM bit streams for performance management and improvement.

G.709 adds the operations, administration, maintenance and provisioning (OAM&P) functionality of SONET/SDH to DWDM optical networks.

Like traditional SONET networks, G.709 optical networks have a layered design (Figure 1-10). This structure enables localized monitoring that helps you isolate and troubleshoot network problems.

Figure 1-10 Optical Transport Network Layers



1.3.2 Optical Channel Layer

The optical channel (OCh) layer is the outermost part of the OTN and spans from client to client. The optical channel is built as follows:

1. A client signal such as SONET, Gigabit Ethernet, IP, asynchronous transfer mode (ATM), fiber channel, or enterprise system connection (ESCON) is mapped to a client payload area and combined with an overhead to create the optical channel payload unit (OPUk).
2. A second overhead is added to the OPUk unit to create the optical channel data unit (ODUk).
3. A third overhead including forward error correction (FEC) is added to the ODUk to create the optical channel transport unit (OTUk).
4. A fourth overhead is added to the OTUk to create the entire OCh layer

1.3.3 Optical Multiplex Section Layer

The optical multiplex section (OMS) of the OTN allows carriers to identify errors occurring within DWDM network sections. The OMS layer consists of a payload and an overhead (OMS-OH). It supports the ability to monitor multiplexed sections of the network, for example the span between an optical multiplexer such as the 3 2MUX-O and a demultiplexer such as the 32 DMX-O.

1.3.4 Optical Transmission Section Layer

The optical transmission section (OTS) layer supports monitoring partial spans of a network's multiplexed sections. This layer consists of a payload and an overhead (OTS-OH). It is a transmission span between two elements in an optical network, such as between:

- a multiplexer such as the 32 MUX-O and an amplifier such as the OPT-PRE;
- an amplifier and another amplifier, such as the OPT-BST and the OPT-PRE;
- or an amplifier such as the OPT-BST and a demultiplexer such as the 32-DMX.

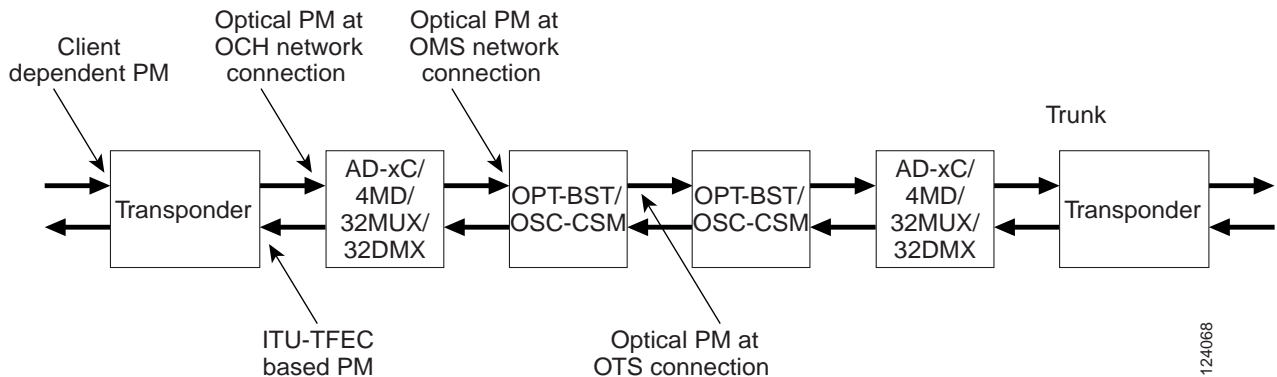
1.3.5 Performance Monitoring Counters and Threshold Crossing Alerts

Performance monitoring (PM) counters and TCAs can be used for identifying trouble and troubleshooting problems in G.709 optical transport networks. ITU-T Recommendation M.2401 recommends that the following PM parameters be monitored at the ODUk Layer:

- SES (severely errored seconds)—A one-second period which contains greater than or equal to 30% errored blocks or at least one defect. SES is a subset of the errored second (ES) parameter, which is a one-second period with one or more errored blocks or at least one defect.
- BBE (background block error counter)—An errored block not occurring as part of an SES. BBE is a subset of the errored block (EB) parameter, which is a block in which one or more bits are in error.

Different performance monitoring count parameters are associated with different read points in a network. [Figure 1-11](#) illustrates the performance monitoring read points that are useful in identifying DWDM circuit points of failure. [Chapter 4, “Performance Monitoring,”](#) lists all PM parameters and provides block diagrams of signal entry points, exit points and interconnections between the individual circuit cards. Consult these specifications to determine which performance monitoring parameters are associated with the system points you want to monitor or provision with CTC or TL1. The monitoring points can vary according to your configuration.

Figure 1-11 Performance Monitoring Points on ONS DWDM



TCAs are used to monitor performance through the management interface by indicating whether preset thresholds have been crossed, or whether a transmission (such as a laser transmission) is degraded. TCAs are not associated with severity levels. They are usually associated with rate, counter, and percentage parameters that are available at transponder monitoring points. [Chapter 4, “Performance Monitoring,”](#) contains more information about these alerts.

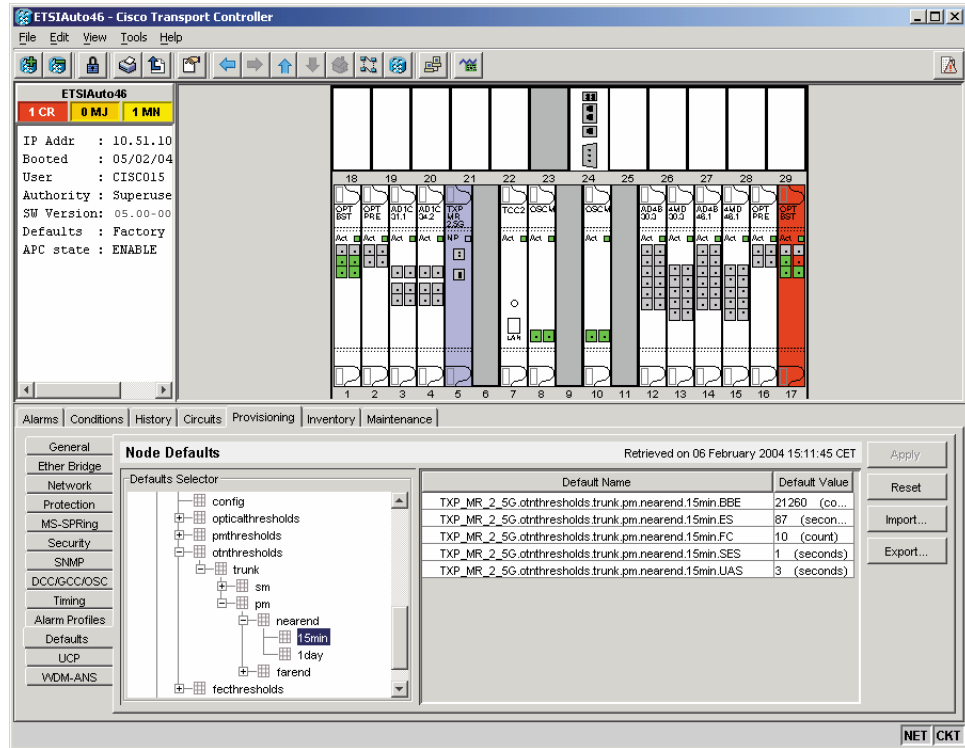
Select and complete the provisioning procedure below according to your network parameters.

Complete the following procedure to provision default node ODUk BBE and SES PM thresholds for TXP cards.

Set Node Default BBE or SES Card Thresholds

-
- Step 1** In node view, click the **Provisioning > Defaults** tabs ([Figure 1-12](#)).

Figure 1-12 Set Default BBE/SES Card Thresholds



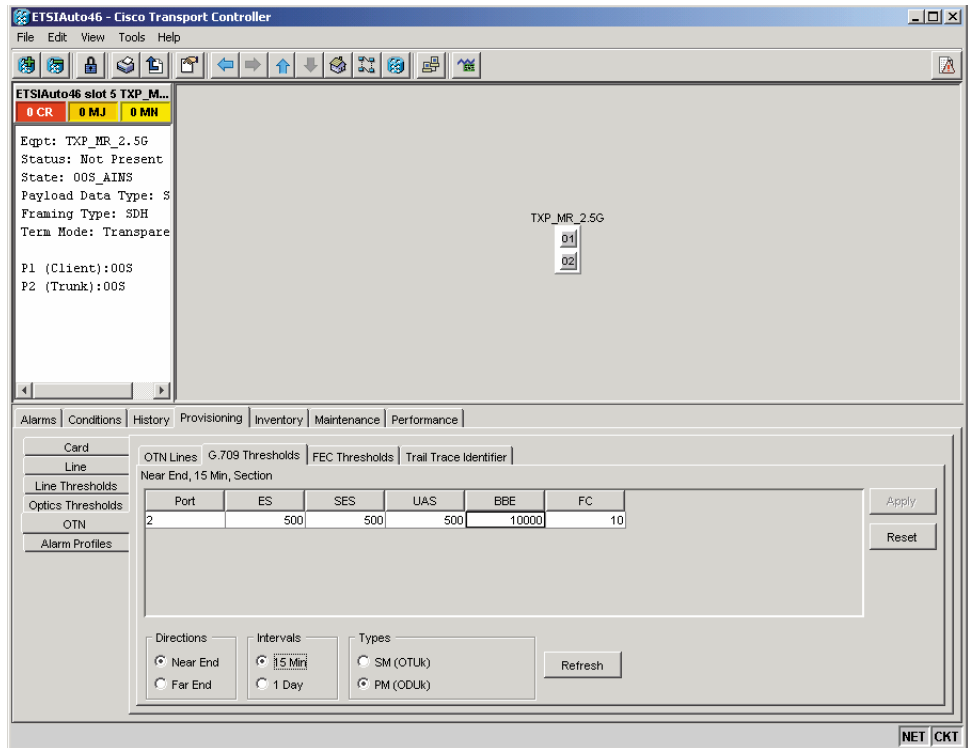
Step 2 In the Defaults Selector field, select Txp_mr_2_5g > otnthresholds > Trunk > pm > 15min.

Complete the following procedure to provision BBE or SES PM thresholds in CTC for an individual TXP card.

Provision Individual Card BBE or SES Thresholds in CTC

- Step 1** In node view, double-click the TXP_MR_2.5G card.
(In this example, other transponder and muxponder cards are also applicable, such as TXP_MR_10G, TXPP_MR_2.5G, and MXP_2.5G_10G.)
- Step 2** Click the **Provisioning > OTN > G.709 Thresholds** tabs (Figure 1-13).

Figure 1-13 Provision Card BBE/SES Thresholds



- Step 3 In the Directions area, click **Near End**.
- Step 4 In the Intervals area, click **15 Min**.
- Step 5 In the Types area, click **PM (ODUk)**.
- Step 6 In the SES and BBE fields, enter threshold numbers, for example 500 and 10000.

Complete the following procedure if you wish to provision PM thresholds in TL1 rather than in CTC.

Provision Card PM Thresholds Using TL1

- Step 1 Open a TL1 command line.
- Step 2 On the TL1 command line, use the following syntax:


```
set-th-{och,clnt}::aid:ctag::montype,thlev,, [tmper];
```

Where:

- The modifier is och, as applicable to the trunk port.
- Montype can be:
 - BBE-PM
 - SES-PM
 - LBCL-MAX

- The thlev parameter is optional and indicates a threshold count value, which is the number of errors which must be exceeded before the threshold is crossed.
- The tmper parameter is optional and is an accumulation time period for performance counters, with possible values of 1-DAY, 1-HR, 1-MIN, 15-MIN, and RAW-DATA.



Note For a list of TL1 commands, refer to the *Cisco ONS 15454 SONET and SDH TL1 Quick Reference Guide, Release 4.7*.

Complete the following procedure to provision TCA thresholds in CTC.

Provision Optical TCA Thresholds

- Step 1** In node view, click the **Provisioning > Optics Thresholds** tabs (Figure 1-14).

Figure 1-14 Provision Optical TCA Thresholds

The screenshot shows the 'Warning Thresholds, 15 Min' configuration page in the CTC interface. The page includes a table of thresholds for various parameters, with the 'Laser Bias High (%)' field highlighted. The 'Types' section has 'TCA' selected, and the 'Intervals' section has '15 Min' selected. A 'Refresh' button is visible.

Line	Port	Laser Bias High (%)	RX Power H...	RX Power L...	TX Power H...	TX Power L...
Line Thresholds	1	81.0	2.0	-20.0	2.0	-7.0
Optics Thresholds	2	81.0	-7.5	-24.5	30.0	-40.0

- Step 2** In the Types area, click **TCA**.
- Step 3** In the Intervals area, click **15 Min**.
- Step 4** In the Laser Bias High (%) field, enter the threshold value, for example, 81.0 percent.

124072

1.3.6 Forward Error Correction

In DWDM spans, FEC reduces the quantities of 3R regeneration needed to maintain signal quality. The following two PM parameters are associated with FEC:

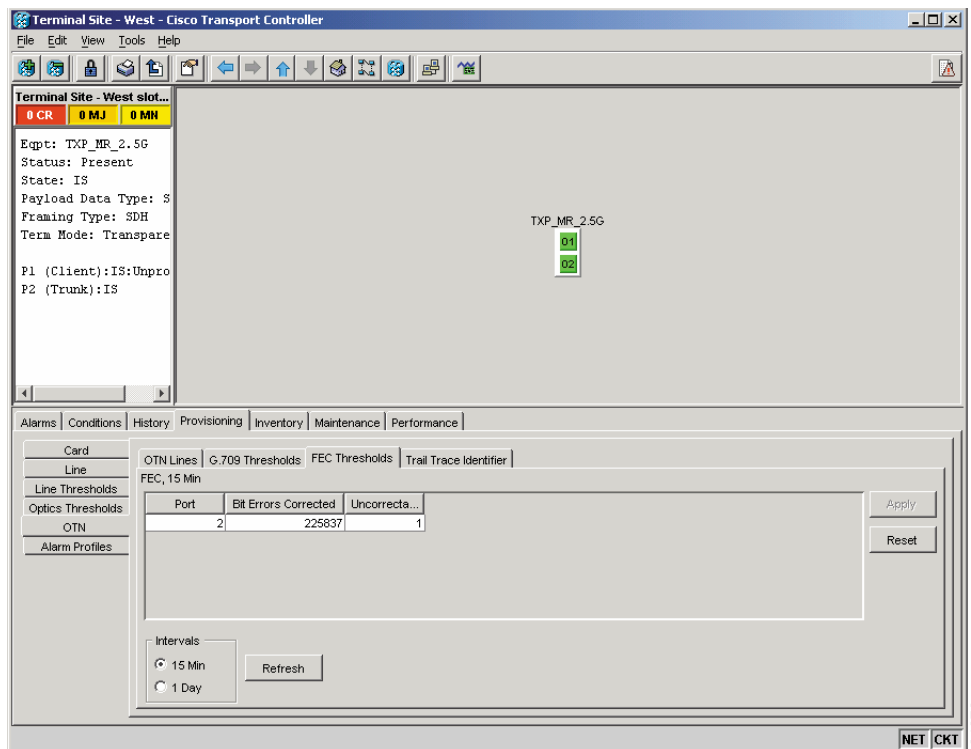
- **BIEC**—Bit errors corrected (BIEC) indicates the number of bit errors corrected in the DWDM trunk line during the PM time interval.
- **UNC-WORDS**—The number of uncorrectable words detected in the DWDM trunk line during the PM time interval.

Complete the following procedure to provision BIEC and UNC-WORDS PM parameters for FEC.

Provision Card FEC Thresholds

- Step 1** In node view, double-click the TXP_MR_2.5G card to open the card view.
(In this example, other transponder and muxponder cards are also applicable, such as TXP_MR_10G, TXPP_MR_2.5G, and MXP_2.5G_10G.)
- Step 2** Click the **Provisioning > OTN > FEC Thresholds** tabs (Figure 1-15).

Figure 1-15 Provisioning Card FEC Thresholds



- Step 3** In the Bit Errors Corrected field, enter a threshold number, for example 225837.
- Step 4** In the Intervals area, click **15 Min**.

1.3.7 Sample Trouble Resolutions

Some sample trouble resolutions using performance monitoring and TCAs for isolating points of degrade are provided below.

Symptom There is a BBE TCA on a single transponder pair.

Possible Cause The transponder input power is out of range.

Recommended Action Check the input power on the transponder. It should be within the specified/supported range.

Possible Cause There are dirty trunk connectors on the transponder.

Recommended Action Check the connector on the trunk port.

Possible Cause There is a degraded trunk patch-cord between the transponder and the DWDM port.

Recommended Action Check the patch-cord on the transponder DWDM port.

Possible Cause There are dirty client connectors on the channel add-drop (ADxC transmit port or the demultiplexer (DMX) has crossed the near-end TCA.

Recommended Action Check the connector on the OCH port of the ADxC.

Possible Cause There are dirty client connectors on the ADxC receive port or the multiplexer (MUX) has crossed the far-end TCA point.

Recommended Action If an optical channel bypass exists along the line, check the connectors.

Symptom There is a BBE TCA on all transponders connected to a band add-drop card (ADxB).

Possible Cause The transponder input power is out of range.

Recommended Action Check the input power on the transponder. It should be within the specified/supported range.

Possible Cause There is a dirty connector on the 4MD port.

Recommended Action Check the connector on the drop port of the ADxB.

Possible Cause There is a dirty connector on the ADxB drop port -and it has crossed the near-end TCA point.

Recommended Action Check the connector on the drop port of the 4MD.

Possible Cause There is a dirty connector on the ADxB add port and it has crossed the far-end TCA.

Recommended Action Check the patch-cord on the 4MD or AD1Bx.

Possible Cause There is a degraded patch-cord between the ADxB and the 4MD.

Recommended Action If an optical band bypass exists along the line, check the band connectors.

Symptom There is a BBE TCA on all transponders which the OCH passes through a single OTS section.

Possible Cause This is not a transponder or channel- related issue.

Recommended Action The problem is in the intercabinet signal path preceding the transponder. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more information about configurations and acceptance tests for this area

Symptom You have an LBC TCA on a single transponder.

Possible Cause The laser of the transponder is degrading.

Recommended Action The problem is within the laser circuitry. Check the OPT-PRE or OPT-BST optical amplifier cards. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more information about setting up these cards.

1.4 Using CTC Diagnostics

In Release 4.7, CTC provides diagnostics for the following functions:

- Verify that card LEDs operate properly.
- Verify that the ASICs on all cards are working.
- Verify the Standby cards are able to handle traffic should a switchover occur.
- Notify the customer of any problems detected via alarms.
- Verify the protection path of a BLSR is operational.

Some of these functions, such as ASIC verification and standby card operation, are invisibly monitored in background functions. Change or problem notifications are provided in the Alarms and Conditions window. Other diagnostic functions—verifying card LED function, creating BLSR diagnostic circuits, and also downloading diagnostic files for technical support—are available to the user in the node view Maintenance > Diagnostic tab. The user-operated diagnostic features are described in the following paragraphs.

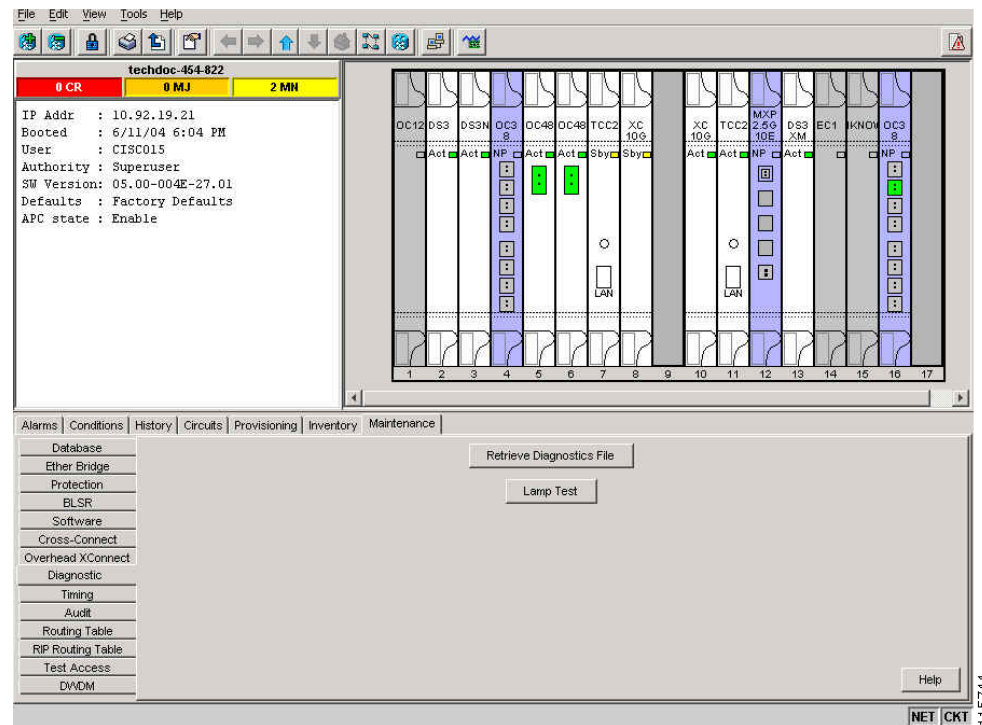
1.4.1 Card LED Lamp Tests

A card LED lamp test determines whether card-level indication LEDs are operational. This diagnostic test is run as part of the initial ONS 15454 turnup, during maintenance routines, or any time you question whether an LED is in working order. Maintenance or higher-level users can complete the following tasks to verify LED operation.

Verify General Card LED Operation

Step 1 In node view, click the **Maintenance > Diagnostic** tab (Figure 1-16).

Figure 1-16 CTC Diagnostic Window



- Step 2** Click **Lamp Test**.
- Step 3** Watch to make sure all the port LEDs illuminate simultaneously for several seconds.
- Step 4** Click **OK** on the Lamp Test Run dialog box.

With the exceptions previously described, if an OC-N or DS-N LED does not light up, the LED is faulty. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).

1.4.2 Retrieve Diagnostics File Button

When you click the Retrieve Diagnostics File button in the Maintenance window, CTC retrieves system data that can be off-loaded by a Maintenance or higher-level user to a local directory and sent to Technical Support for troubleshooting purposes. The diagnostics file is in machine language and is not human-readable, but can be used by Cisco Technical Support for problem analysis. Complete the following task to off-load the diagnostics file.



Note

In addition to the machine-readable diagnostics file, the ONS 15454 also stores an audit trail of all system events such as user logins, remote logins, configuration, and changes. This audit trail is considered a record-keeping feature rather than a troubleshooting feature. Information about the feature is located in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

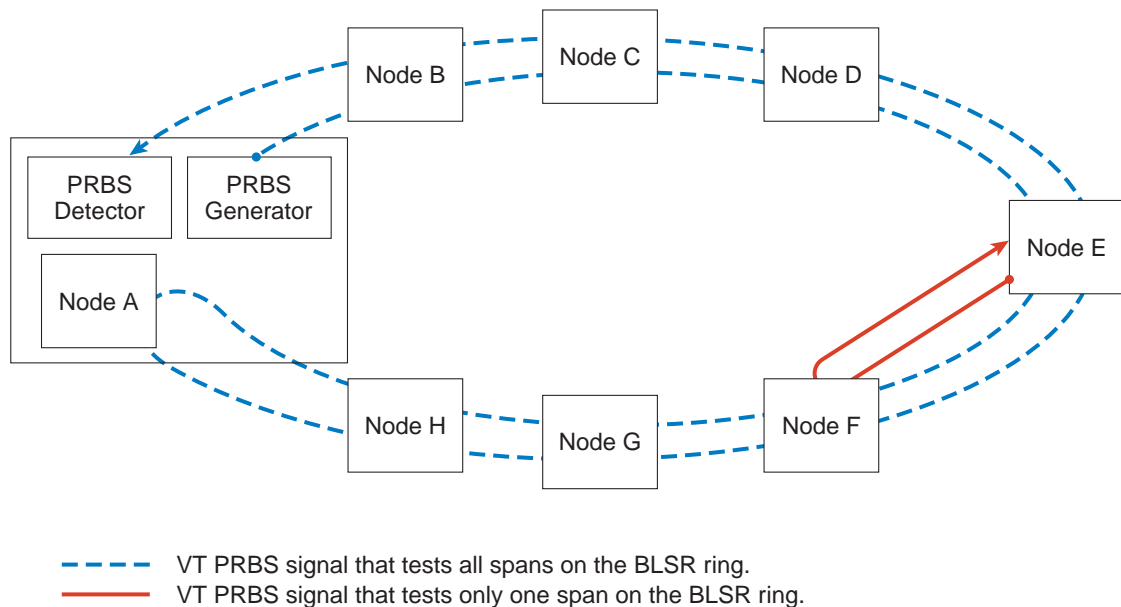
Off-Load the Diagnostics File

-
- Step 1** In the node view, click the **Maintenance > Diagnostic** tab (Figure 1-16).
- Step 2** Click **Retrieve Diagnostics File**.
- Step 3** In the Saving Diagnostic File dialog box, navigate to the directory (local or network) where you want to save the file.
- Step 4** Enter a name in the File Name field.
- You do not have to give the archive file a particular extension. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.
- Step 5** Click **Save**.
- The Get Diagnostics status window shows a progress bar indicating the percentage of the file being saved, then shows “Get Diagnostics Complete.”
- Step 6** Click **OK**.
-

1.4.3 BLSR Diagnostic Circuit

In Release 5.0, CTC provides a diagnostic BLSR loopback circuit feature that uses pseudo-random bit sequence (PRBS) error detection to monitor standby circuit path readiness. The diagnostic circuit originates and terminates on a single node, where the signal result is detected and analyzed for errors. The circuit can be configured for an end-to-end or multiple-node path layout, traversing the transmit and receive standby paths as shown in Figure 1-17.

Figure 1-17 CTC Node View Diagnostic Window



NOTE: The end without the arrow is where the PRBS pattern is generated. The end with the arrow is the end where the PRBS pattern is detected.

115747

Each card type utilizes the diagnostic feature differently. Standby electrical cards run PRBS tests to ensure signal path integrity. Optical cards do not run PRBS tests, but instead run ASIC tests to test card operability. Cross-connect cards verify the standby BLSR paths.

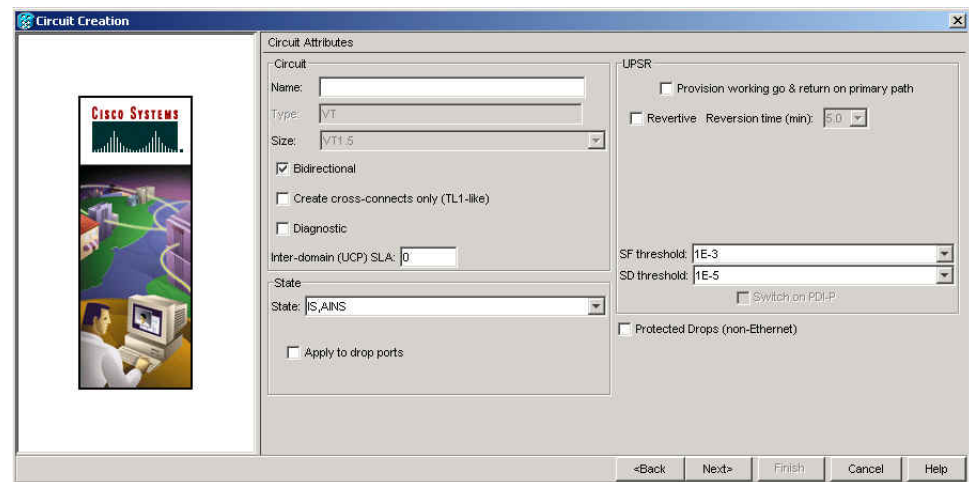
A diagnostic BLSR circuit is created much the same way as a normal standby PCA circuit but is designated by checking the Diagnostic checkbox during circuit creation. A normal circuit uses line cards as the endpoints, but if a circuit is configured as a diagnostic the endpoints are cross-connect cards.

In Release 5.0, the maximum diagnostic circuit size is VT1.5. The circuit can only be created if the same STS is available on each span the circuit traverses. Only one BLSR diagnostic circuit can be sourced and detected per node. When you use a BLSR diagnostic that traverses one or more intermediate nodes, create or utilize an existing bidirectional circuit on each intermediate node. At the terminating node, you will need to create a

Create a BLSR Diagnostic Circuit

- Step 1** Log into the node where you will create the diagnostic circuit.
- Step 2** If you want to assign a name to the circuit source and destination ports before you create the circuit, refer to the task for assigning a name to a port in the *Cisco ONS 15454 Procedure Guide*. If not, continue with [Step 3](#).
- Step 3** From the View menu, choose **Go to Network View**.
- Step 4** Click the **Circuits** tab, then click **Create**.
- Step 5** In the Circuit Creation dialog box, complete the following fields:
 - Circuit Type—Choose **VT**.
 - Number of Circuits—Type the number of circuits you want to create. The default is 1.
 - Auto-ranged—Uncheck the box.
- Step 6** Click **Next**.
- Step 7** Define the circuit attributes in the Circuit Creation Dialog Box shown in [Figure 1-18](#) using the following parameters:

Figure 1-18 Network View Circuit Creation Dialog Box



115954

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters, (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—VT1.5 is the default. You cannot change it.
- Bidirectional—This is the default value. Leave it checked for this circuit.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
 - IS—Places the circuit cross-connects in the IS-NR service state.
 - OOS,DSBLD—Places the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
 - IS,AINS—Places the circuit cross-connects in the Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
 - OOS,MT—Places the circuit cross-connects in the OOS-MA,MT service state. This service state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use the OOS,MT administrative state for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. For instructions and information about administrative and service states, refer to the *Cisco ONS 15454 Procedure Guide*.



Note If VT circuit source and destination ports are in an OOS-AU,AINS; OOS-MA,MT; or IS-NR service state, VT circuit connections in OOS-AU,AINS change to IS-NR even if a physical signal is not present. Refer to the *Cisco ONS 15454 Reference Manual* for more information.

- Diagnostic—Check this box to create a diagnostic circuit.
- Apply to drop ports—Check this box if you want to apply the service state chosen in the State field to the circuit source and destination ports. If the box is unchecked, CTC does not change the state of the source and destination ports. The circuit bandwidth is the same as the port bandwidth. If the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. For the requirements necessary to apply a service state to drop ports, refer to the *Cisco ONS 15454 Reference Manual*.



Note LOS alarms are generated if in service (IS-NR) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Disabled for a diagnostic circuit.
- Inter-domain (UCP) SLA—Disabled for a diagnostic circuit.
- Protected Drops—Disabled for a diagnostic circuit.

Step 8 Click **Next**.

Step 9 In the Source area of the Circuit Creation pane, complete the following:

- a. From the Node pull-down menu, choose the node.
- b. From the Slot pull-down menu, choose **PRBS Generator**.
- c. Click **Next**.

- Step 10** In the Destination area of the Circuit Creation pane, complete the following:
- From the Node pull-down menu, choose the node. The only selectable item in the list is the node chosen as the source node.
 - From the Slot pull-down menu, choose the slot where the BLSR span originates.
 - From the STS pull-down menu, choose the STS.
 - From the VT pull-down menu, choose the VT.
 - Click **Next**.
- Step 11** Click **Finish**. One of the following results occurs, depending on the circuit properties you chose in the Circuit Creation dialog box:
- If you entered more than 1 in the Number of Circuits field and selected Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto-ranging. After completing the circuit(s), the Circuits window appears.
 - If you entered more than 1 in the Number of Circuits field and did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 10 for each additional circuit. After completing the circuit(s), the Circuits window appears.
- Step 12** In the Circuits window, verify that the new circuit(s) appear in the circuits list.
-

1.5 Restoring the Database and Default Settings

This section contains troubleshooting for node operation errors that require restoration of software data or the default node setup.

1.5.1 Restore the Node Database

Symptom One or more nodes are not functioning properly or have incorrect data.

Possible Cause There is an incorrect or corrupted node database.

Recommended Action Perform a Restore the Database procedure. Refer to the [“Restore the Database” procedure on page 1-33](#).

Restore the Database



Caution


E1000-2 cards lose traffic for approximately 90 seconds when an ONS 15454 database is restored. Traffic is lost during the period of spanning tree reconvergence. The [“CARLOSS \(E100T, E1000F\)” alarm on page 2-46](#) appears and clears during this period.

**Caution**

If you are restoring the database on multiple nodes, wait approximately one minute after the TCC2 reboot has completed on each node before proceeding to the next node

**Note**

The following parameters are not backed up and restored: node name, IP address, subnet mask and gateway, and Internet Inter-ORB Protocol (IIOP) port. If you change the node name and then restore a backed up database with a different node name, the circuits map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

- Step 1** In CTC, log into the node where you will restore the database:
- On the PC connected to the ONS 15454, start Netscape or Internet Explorer.
 - In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15454 IP address.
A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to an ONS 15454, this process can take several minutes. After the download, the CTC Login dialog box appears.
 - In the Login dialog box, type a user name and password (both are case sensitive) and click **Login**. The CTC node view window appears.
- Step 2** Ensure that no ring or span (four-fiber only) switch events are present; for example, ring-switch east or west and span-switch east or west. In network view, click the **Conditions** tab and click **Retrieve** to view a list of conditions.
- Step 3** If switch events need to be cleared, in node view click the **Maintenance > BLSR** tab and view the West Switch and East Switch columns.
- If a switch event (not caused by a line failure) is present, choose **CLEAR** from the pull-down menu and click **Apply**.
 - If a switch event caused by the Wait to Restore (WTR) condition is present, choose **LOCKOUT SPAN** from the pull-down menu and click **Apply**. When the LOCKOUT SPAN is applied, choose **CLEAR** from the pull-down menu and click **Apply**.
- Step 4** In node view, click the **Maintenance > Database** tab.
- Step 5** Click **Restore**.
- Step 6** Locate the database file stored on the workstation hard drive or on network storage.
-  **Note** To clear all existing provisioning, locate and upload the database found on the latest ONS 15454 software CD.
- Step 7** Click the database file to highlight it.
- Step 8** Click **Open**. The DB Restore dialog box appears. Opening a restore file from another node or from an earlier backup might affect traffic on the login node.
- Step 9** Click **Yes**.
The Restore Database dialog box monitors the file transfer.
- Step 10** Wait for the file to complete the transfer to the TCC2.

- Step 11** Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears. Wait for the node to reconnect.
- Step 12** If you cleared a switch in [Step 3](#), reapply the switch as needed.
-

1.5.2 Restore the Node to Factory Configuration

Symptom A node has both TCC2 cards in standby state, and you are unable reset the TCC2 cards to make the node functional.

Possible Cause Both TCC2 cards are failing in the node.

Possible Cause You are replacing both TCC2 cards at the same time.

Recommended Action Restore the node to factory configuration. Refer to the [“Use the Reinitialization Tool to Clear the Database and Upload Software \(Windows\)”](#) procedure on page 1-36 or the [“Use the Reinitialization Tool to Clear the Database and Upload Software \(UNIX\)”](#) procedure on page 1-37 as required.



Caution

Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinit tool chooses the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You might accidentally copy an incorrect database if multiple databases are kept in the specified directory.



Caution

Restoring a node to the factory configuration deletes all cross-connects on the node.



Caution

If you are restoring the database on multiple nodes, wait until the TCC2 cards have rebooted on each node before proceeding to the next node.



Caution

Restoring a node to factory configuration on a Windows or UNIX workstation should only be carried out on a standby TCC2 card.



Caution

Cisco recommends that you take care to save the node database to a safe location if you will not be restoring the node using the database provided on the software CD.



Note

The following parameters are not backed up and restored when you delete the database and restore the factory settings: node name, IP address, subnet mask and gateway, and IIOP port. If you change the node name and then restore a backed up database with a different node name, the circuits map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

**Note**

If the software package files and database backup files are located in different directories, complete the Package and Database fields (Figure 1-19 on page 1-36).

**Note**

If you need to install or replace one or more TCC2 cards, refer to the *Cisco ONS 15454 Procedure Guide* for installation instructions.

Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

**Caution**

Restoring a node to the factory configuration deletes all cross-connects on the node.

**Caution**

Restoring a node to factory configuration on a Windows workstation should only be carried out on a standby TCC2 card.

**Note**

The TCC2 cards reboot several times during this procedure. Wait until they are completely rebooted before continuing.

- Step 1** Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.
- Step 2** To find the recovery tool file, go to **Start > Run > Browse** and select the CD drive.
- Step 3** On the CD drive, go to the CISCO15454 folder and choose **All Files from the Files of Type** pull-down menu.
- Step 4** Select the RE-INIT.jar file and click **Open** to open the reinit tool (Figure 1-19).

Figure 1-19 Reinitialization Tool in Windows

The screenshot shows the Reinitialization Tool interface. At the top, there are input fields for GNE IP, Node IP, Username (CISCO15), and Password. Below these are several checkboxes: Upload Package?, Force upload?, Activate/Revert?, Re-init database?, and Confirm?. A search path is entered: auto\otsrc-sw\w\patriot_throttle\PATRIOT_THROTTLE_SSIT_94_CD\CD15454\Cisco15454. There are 'Browse...' buttons for Package, Database, and Node version. Package type, Package version, Elapsed, and Time to copy fields are also present. A progress bar shows 0% completion. At the bottom, there are 'Go' and 'Quit' buttons. A small vertical text '110725' is visible on the right side of the screenshot.

- Step 5** If the node you are reinitializing is an end network element (ENE) in a proxy server network, enter the IP address of the gateway network element (GNE) in the GNE IP field. If not, leave it blank.
- Step 6** Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-19).
- Step 7** If the User ID field does not contain your user ID, enter the ID. Enter your password in the Password field.
- Step 8** Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If one is not checked, check the check box.

- Step 9** If you are uploading the same version of software that is already active (for example, you are trying to upload version 4.7 when version 4.7 is already active), check the Force Upload checkbox. This option forces the NE to have the same software version on the working and protect flash memory.



Note The Force Upload box is only applicable when the Upload Package checkbox is checked.

- Step 10** In the Search Path field, verify that the path to the CISCO15454 folder on the CD drive is listed.



Caution Before you perform the next step, be sure you are uploading the correct database. You cannot reverse the upload process after you click Yes.

- Step 11** Click **Go**. A confirmation dialog box appears.

- Step 12** Click **Yes**.

- Step 13** The status bar at the bottom of the screen displays Complete when the node has activated the software and uploaded the database.



Note The Complete message only indicates that the TCC2 successfully uploaded the database, not that the database restore was successful. The TCC2 then tries to restore the database after it reboots.

- Step 14** If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the TCC2 card or on the hub or switch to which the ONS 15454 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC.

- Step 15** Manually set the node name and network configuration to site-specific values. See the *Cisco ONS 15454 DWDM Installation and Operations Guide* for information about setting the node name, IP address, mask and gateway, and IIOP port.

Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)



Caution Restoring a node to the factory configuration deletes all cross-connects on the node.



Caution Restoring a node to factory configuration on a UNIX workstation should only be carried out on a standby TCC2 card.



Note The TCC2 cards reboot several times during this procedure. Wait until they are completely rebooted before continuing.



Note Java Runtime Environment (JRE) 1.03_02 must also be installed on the computer you use to perform this procedure.

- Step 1** Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.
- Step 2** To find the recovery tool file, go to the CISCO15454 directory on the CD (usually /cdrom/cdrom0/CISCO15454).
- Step 3** If you are using a file explorer, double-click the **RE-INIT.jar** file to open the reinit tool (Figure 1-20). If you are working with a command line interface, run **java -jar RE-INIT.jar**.

Figure 1-20 Reinitialization Tool in UNIX

- Step 4** If the node you are reinitializing is an ENE in a proxy server network, enter the IP address of the GNE in the GNE IP field. If not, leave it blank.
- Step 5** Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-20).
- Step 6** If the User ID field does not contain your user ID, enter the ID. Enter your password in the Password field.
- Step 7** Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If one is not checked, check the check box.
- Step 8** If you are uploading the same version of software that is already active (for example, you are trying to upload version 4.7 when version 4.7 is already active), check the Force Upload checkbox. This option forces the NE to have the same software version on the working and protect flash memory.
- Step 9** In the Search Path field, verify that the path to the CISCO15454 folder on the CD-ROM drive is listed.



Caution

Before you perform the next step, be sure you are uploading the correct database. You cannot reverse the upload process after you click Yes.

- Step 10** Click **Go**. A confirmation dialog box appears.
- Step 11** Click **Yes**.
- Step 12** The status bar at the bottom of the screen displays Complete when the node has activated the software and uploaded the database.



Note

The Complete message only indicates that the TCC2 successfully uploaded the database; not that the database restore was successful. The TCC2 then tries to restore the database after it reboots.

- Step 13** If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the TCC2 card or on the hub or switch where the ONS 15454 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC.

- Step 14** Set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15454 Procedure Guide* for information about provisioning the node name, IP address, subnet mask and gateway, and IIOP port.
-

1.6 PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and JREs for R4.7, and troubleshooting procedures for PC and network connectivity to the ONS 15454.

1.6.1 PC System Minimum Requirements

Workstations running CTC R4.7 for the ONS products on Windows platforms need to have the following minimum requirements:

- Pentium III or higher processor
- Processor speed of at least 700 MHz
- 256 Mb or more of RAM
- 50 Mb or more of available hard disk space
- 20 GB or larger hard drive

1.6.2 Sun System Minimum Requirements

Workstations running CTC R4.7 for the ONS products on Sun workstations need to have the following minimum requirements:

- UltraSPARC or faster processor
- 256 Mb or more of RAM
- 50 Mb or more of available hard disk space

1.6.3 Supported Platforms, Browsers, and JREs

Software R4.7 CTC supports the following platforms:

- Windows NT
- Windows 98
- Windows XP
- Windows 2000
- Solaris 8
- Solaris 9

Software R4.7 CTC supports the following browsers and JREs:

- Netscape 4.76 (on Solaris 8 or 9 with Java plug-in 1.3.1)
- Netscape 7 (on Solaris 8 or 9 with Java plug-in 1.4)

- PC platforms with Java plug-in 1.3.1 or 1.4
- Internet Explorer 6.0 (on PC platforms with Java plug-in 1.3.1 or 1.4)

**Note**

You can obtain browsers at the following URLs:

Netscape: <http://channels.netscape.com/ns/browsers/default.jsp>

Internet Explorer: <http://www.microsoft.com>

**Note**

The recommended JRE version is JRE 1.4.2.

**Note**

JRE 1.4.2 for Windows and Solaris is available on R4.7 product CDs.

1.6.4 Unsupported Platforms and Browsers

Software R4.7 does not support the following platforms:

- Windows 95
- Solaris 2.5
- Solaris 2.6

Software R4.7 does not support the following browsers and JREs:

- Netscape 4.73 for Windows.
- Netscape 4.76 on Solaris is not supported except when used with JRE 1.3.1.
- JRE 1.4.2 is not supported except with Netscape 7 on Solaris 8 or 9.

1.6.5 Unable to Verify the IP Configuration of Your PC

Symptom When connecting your PC to the ONS 15454, you are unable to successfully ping the IP address of your PC to verify the IP configuration.


Possible Cause The IP address was typed incorrectly.

Recommended Action Verify that the IP address used to ping the PC matches the IP address displayed when in the Windows IP Configuration information retrieved from the system. See the “[Verify the IP Configuration of Your PC](#)” procedure on page 1-41.

Possible Cause The IP configuration of your PC is not properly set.

Recommended Action Verify the IP configuration of your PC. Complete the “[Verify the IP Configuration of Your PC](#)” procedure on page 1-41. If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC.

Verify the IP Configuration of Your PC

-
- Step 1** Open a DOS command window by selecting **Start > Run** from the Start menu.
- Step 2** In the Open field, type **command** and then click **OK**. The DOS command window appears.
- Step 3** At the prompt in the DOS window, type one of the following commands:
- For Windows 98, NT, and 2000, type **ipconfig** and press the **Enter** key.
- The Windows IP configuration information appears, including the IP address, subnet mask, and the default gateway.
-  **Note** The winipcfg command only returns the information above if you are on a network.
-
- Step 4** At the prompt in the DOS window, type **ping** followed by the IP address shown in the Windows IP configuration information previously displayed.
- Step 5** Press the **Enter** key to execute the command.
- If the DOS window returns multiple (usually four) replies, the IP configuration is working properly. If you do not receive a reply, your IP configuration might not be properly set. Contact your Network Administrator for instructions to correct the IP configuration of your PC.
-

1.6.6 Browser Login Does Not Launch Java

Symptom The message “Loading Java Applet” does not appear and the JRE does not launch during the initial login.

Possible Cause The PC operating system and browser are not properly configured.

Recommended Action Reconfigure the PC operating system java plug-in control panel and the browser settings. Complete the [“Reconfigure the PC Operating System Java Plug-in Control Panel” procedure on page 1-41](#) and the [“Reconfigure the Browser” procedure on page 1-42](#).

Reconfigure the PC Operating System Java Plug-in Control Panel

-
- Step 1** From the Windows start menu, click **Settings > Control Panel**.
- Step 2** If **Java Plug-in** does not appear, the JRE might not be installed on your PC.
- Run the Cisco ONS 15454 software CD.
 - Open the *CD-drive:\Windows\JRE* folder.
 - Double-click the **j2re-1_4_2-win** icon to run the JRE installation wizard.
 - Follow the JRE installation wizard steps.
- Step 3** From the Windows start menu, click **Settings > Control Panel**.
- Step 4** In the Java Plug-in Control Panel window, double-click the **Java Plug-in 1.4.2** icon.
- Step 5** Click the **Advanced** tab on the Java Plug-in Control Panel.

- Step 6** Navigate to **C:\ProgramFiles\JavaSoft\JRE\1.4.2**.
- Step 7** Select **JRE 1.4**.
- Step 8** Click **Apply**.
- Step 9** Close the Java Plug-in Control Panel window.
-

Reconfigure the Browser

- Step 1** From the Start Menu, launch your browser application.
- Step 2** If you are using Netscape Navigator:
- On the Netscape Navigator menu bar, click the **Edit > Preferences** menus.
 - In the Preferences window, click the **Advanced > Proxies** categories.
 - In the Proxies window, click the **Direct connection to the Internet** check box and click **OK**.
 - On the Netscape Navigator menu bar, click the **Edit > Preferences** menus.
 - In the Preferences window, click the **Advanced > Cache** categories.
 - Confirm that the Disk Cache Folder field shows one of the following paths:
 - For Windows 98/ME, **C:\ProgramFiles\Netscape\Communicator\cache**
 - For Windows NT/2000, **C:\ProgramFiles\Netscape\username\Communicator\cache**.
 - If the Disk Cache Folder field is not correct, click **Choose Folder**.
 - Navigate to the file listed in Step f, and click **OK**.
 - Click **OK** on the Preferences window and exit the browser.
- Step 3** If you are using Internet Explorer:
- On the Internet Explorer menu bar, click the **Tools > Internet Options** menus.
 - In the Internet Options window, click the **Advanced** tab.
 - In the Settings menu, scroll down to Java (Sun) and click the **Use Java 2 v1.4.2 for applet (requires restart)** check box.
 - Click **OK** in the Internet Options window and exit the browser.
- Step 4** Temporarily disable any virus-scanning software on the computer. See the [“Browser Stalls When Downloading CTC JAR Files From TCC2”](#) section on page 1-47.
- Step 5** Verify that the computer does not have two network interface cards (NICs) installed. If the computer does have two NICs, remove one.
- Step 6** Restart the browser and log on to the ONS 15454.
-

1.6.7 Unable to Verify the NIC Connection on Your PC

Symptom When connecting your PC to the ONS 15454, you are unable to verify the NIC connection is working properly because the link LED is not illuminated or flashing.

Possible Cause The CAT-5 cable is not plugged in properly.

Recommended Action Confirm that both ends of the cable are properly inserted. If the cable is not fully inserted due to a broken locking clip, the cable should be replaced.

Possible Cause The CAT-5 cable is damaged.

Recommended Action Ensure that the cable is in good condition. If in doubt, use a known-good cable. Often, cabling is damaged due to pulling or bending.

Possible Cause Incorrect type of CAT-5 cable is being used.

Recommended Action If connecting an ONS 15454 directly to your laptop, a PC, or a router, use a straight-through CAT-5 cable. When connecting the ONS 15454 to a hub or a LAN switch, use a crossover CAT-5 cable. For details on the types of CAT-5 cables, see the [“Crimp Replacement LAN Cables” section on page 1-65](#).

Possible Cause The NIC is improperly inserted or installed.

Recommended Action If you are using a Personal Computer Memory Card International Association (PCMCIA)-based NIC, remove and reinsert the NIC to make sure the NIC is fully inserted. (If the NIC is built into the laptop or PC, verify that the NIC is not faulty.)

Possible Cause The NIC is faulty.

Recommended Action Confirm that the NIC is working properly. If you have no issues connecting to the network (or any other node), then the NIC should be working correctly. If you have difficulty connecting a to the network (or any other node), then the NIC might be faulty and needs to be replaced.

1.6.8 Verify PC Connection to the ONS 15454 (ping)

Symptom The TCP/IP connection was established and then lost.

Possible Cause A lost connection between the PC and the ONS 15454.

Recommended Action Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 TCC2 card. A ping command should work if the PC connects directly to the TCC2 card or uses a LAN to access the TCC2 card. Complete the [“Ping the ONS 15454” procedure on page 1-44](#).

Ping the ONS 15454

-
- Step 1** Display the command prompt:
- If you are using a Microsoft Windows operating system, from the Start Menu choose **Run**, type **command** in the Open field of the Run dialog box, and click **OK**.
 - If you are using a Sun Solaris operating system, from the Common Desktop Environment (CDE) click the **Personal Application tab** and click **Terminal**.
- Step 2** For both the Sun and Microsoft operating systems, at the prompt type:
- ```
ping ONS-15454-IP-address
```
- For example:
- ```
ping 198.168.10.10
```
- Step 3** If the workstation has connectivity to the ONS 15454, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a “Request timed out” message appears.
- Step 4** If the ping is successful, an active TCP/IP connection exists. Restart CTC.
- Step 5** If the ping is not successful, and the workstation connects to the ONS 15454 through a LAN, check that the workstation’s IP address is on the same subnet as the ONS node.
- Step 6** If the ping is not successful and the workstation connects directly to the ONS 15454, check that the link light on the workstation’s NIC is illuminated.
-

1.6.9 Unknown Node IP Address

Symptom The IP address of the node is unknown and you are unable to login.

Possible Cause The node is not set to the default IP address.

Recommended Action Leave one TCC2 card in the shelf. Connect a PC directly to the remaining TCC2 card and perform a hardware reset of the card. The TCC2 card transmits the IP address after the reset to enable you to capture the IP address for login. Complete the [“Retrieve Unknown Node IP Address” procedure on page 1-44](#).

Retrieve Unknown Node IP Address

-
- Step 1** Connect your PC directly to the active TCC2 card Ethernet port on the faceplate.
- Step 2** Start the Sniffer application on your PC.
- Step 3** Perform a hardware reset by pulling and reseating the active TCC2 card.
- Step 4** After the TCC2 card completes resetting, it broadcasts its IP address. The Sniffer software on your PC will capture the IP address being broadcast.
-

1.7 CTC Operation Troubleshooting

This section contains troubleshooting procedures for CTC login or operation problems.

1.7.1 CTC Colors Do Not Appear Correctly on a UNIX Workstation

Symptom When running CTC on a UNIX workstation, the colors do not appear correctly. For example, both major and minor alarms appear in the same color.

Possible Cause When running in 256-color mode on a UNIX workstation, color-intensive applications such as Netscape might use all of the colors.

Recommended Action CTC requires a full 24-color palette to run properly. When logging into CTC on a UNIX workstation, run as many colors as your adapter will support. In addition, you can use the `-install` or the `-ncols 32` command line options to limit the number of colors that Netscape uses. Complete the [“Limit Netscape Colors” procedure on page 1-45](#). If the problem persists after limiting Netscape colors, exit any other color-intensive applications in use.

Limit Netscape Colors

Step 1 Close the current session of Netscape.

Step 2 Launch Netscape from the command line by typing:

```
netscape -install (installs Netscape colors for Netscape use)
```

or

```
netscape -ncols 32 (limits Netscape to 32 colors so that if the requested color is not available,  
Netscape chooses the closest color option)
```

1.7.2 Unable to Launch CTC Help After Removing Netscape

Symptom After removing Netscape and running CTC using Internet Explorer, you are unable to launch CTC Help and receive an “MSIE is not the default browser” error message.

Possible Cause Loss of association between browser and Help files.

Recommended Action When the CTC software and Netscape are installed, the Help files are associated with Netscape by default. When you remove Netscape, the Help files are not automatically associated with Internet Explorer as the default browser. Reset Internet Explorer as the default browser so that CTC associates the Help files to the correct browser. Complete the [“Reset Internet Explorer as the Default Browser for CTC” procedure on page 1-46](#) to associate the CTC Help files to the correct browser.

Reset Internet Explorer as the Default Browser for CTC

-
- Step 1 Open the Internet Explorer browser.
 - Step 2 From the menu bar, click **Tools > Internet Options**. The Internet Options window appears.
 - Step 3 In the Internet Options window, click the **Programs** tab.
 - Step 4 Click the **Internet Explorer should check to see whether it is the default browser** check box.
 - Step 5 Click **OK**.
 - Step 6 Exit any and all open and running CTC and Internet Explorer applications.
 - Step 7 Launch Internet Explorer and open a new CTC session. You should now be able to access the CTC Help.
-

1.7.3 Unable to Change Node View to Network View

Symptom When activating a large, multinode BLSR from Software R3.2 to Software R3.3, some of the nodes appear grayed out. Logging into the new CTC, the user is unable to change node view to network view on any and all nodes, from any workstation. This is accompanied by an “Exception occurred during event dispatching: java.lang.OutOfMemoryError” in the java window.

Possible Cause The large, multinode BLSR requires more memory for the graphical user interface (GUI) environment variables.

Recommended Action Reset the system or user CTC_HEAP environment variable to increase the memory limits. Complete the [“Reset the CTC_HEAP Environment Variable for Windows” procedure on page 1-46](#) or the [“Reset the CTC_HEAP Environment Variable for Solaris” procedure on page 1-47](#) to enable the CTC_HEAP variable change.



Note This problem typically affects large networks where additional memory is required to manage large numbers of nodes and circuits.

Reset the CTC_HEAP Environment Variable for Windows

-
- Step 1 Exit any and all open and running CTC and Netscape applications.
 - Step 2 From the Windows Desktop, right-click My Computer and choose **Properties** in the shortcut menu.
 - Step 3 In the System Properties window, click the **Advanced** tab.
 - Step 4 Click **Environment Variables** to open the Environment Variables window.
 - Step 5 Click **New** under the User variables field or the System variables field.
 - Step 6 Type **CTC_HEAP** in the Variable Name field.
 - Step 7 Type **256** in the Variable Value field, and then click **OK** to create the variable.
 - Step 8 Click **OK** in the Environment Variables window to accept the changes.
 - Step 9 Click **OK** in the System Properties window to accept the changes.

Restart the browser and CTC software.

Reset the CTC_HEAP Environment Variable for Solaris

- Step 1 From the user shell window, kill any CTC applications.
 - Step 2 Kill any Netscape applications.
 - Step 3 In the user shell window, set the environment variable to increase the heap size:

```
% setenv CTC_HEAP 256
```
 - Step 4 Restart the browser and CTC software in the same user shell window.
-

1.7.4 Browser Stalls When Downloading CTC JAR Files From TCC2

Symptom The browser stalls or hangs when downloading a CTC JAR file from the TCC2 card.

Possible Cause McAfee VirusScan software might be interfering with the operation. The problem occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or later.

Recommended Action Disable the VirusScan Download Scan feature. Complete the [“Disable the VirusScan Download Scan”](#) procedure on page 1-47.

Disable the VirusScan Download Scan

- Step 1 From the Windows Start menu, choose **Programs > Network Associates > VirusScan Console**.
 - Step 2 Double-click the **VShield** icon listed in the VirusScan Console dialog box.
 - Step 3 Click **Configure** on the lower part of the Task Properties window.
 - Step 4 Click the **Download Scan** icon on the left of the System Scan Properties dialog box.
 - Step 5 Uncheck the **Enable Internet download scanning** check box.
 - Step 6 Click **Yes** when the warning message appears.
 - Step 7 Click **OK** in the System Scan Properties dialog box.
 - Step 8 Click **OK** in the Task Properties window.
 - Step 9 Close the McAfee VirusScan window.
-

1.7.5 CTC Does Not Launch

Symptom CTC does not launch; usually an error message appears before the login window appears.

Possible Cause The Netscape browser cache might point to an invalid directory.

Recommended Action Redirect the Netscape cache to a valid directory. Complete the [“Redirect the Netscape Cache to a Valid Directory”](#) procedure on page 1-48.

Redirect the Netscape Cache to a Valid Directory

-
- Step 1 Launch Netscape.
 - Step 2 open the **Edit** menu.
 - Step 3 Choose **Preferences**.
 - Step 4 Under the Category column on the left side, expand the **Advanced** category and choose the **Cache** tab.
 - Step 5 Change your disk cache folder to point to the cache file location.

The cache file location is usually C:\ProgramFiles\Netscape\Users\yourname\cache. The *yourname* segment of the file location is often the same as the user name.

1.7.6 Slow CTC Operation or Login Problems

Symptom You experience slow CTC operation or have problems logging into CTC.

Possible Cause The CTC cache file might be corrupted or might need to be replaced.

Recommended Action Delete the CTC cache file. This operation forces the ONS 15454 to download a new set of JAR files to your computer hard drive. Complete the [“Delete the CTC Cache File Automatically”](#) procedure on page 1-48 or the [“Delete the CTC Cache File Manually”](#) procedure on page 1-49.

Delete the CTC Cache File Automatically



Caution

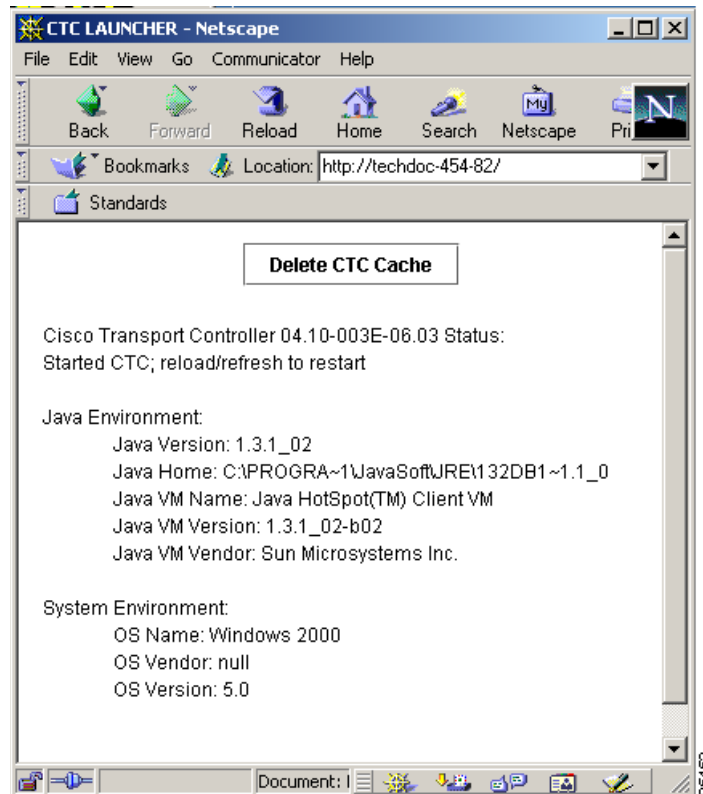
All running sessions of CTC must be halted before deleting the CTC cache. Deleting CTC cache might cause any CTC running on this system to behave in an unexpected manner.

-
- Step 1 Enter an ONS 15454 IP address into the browser URL field. The initial browser window shows a **Delete CTC Cache** button.
 - Step 2 Close all open CTC sessions and browser windows. The PC operating system does not allow you to delete files that are in use.
 - Step 3 Click **Delete CTC Cache** on the initial browser window to clear the CTC cache. [Figure 1-21](#) shows the Delete CTC Cache window.



Note For CTC releases earlier than R3.0, automatic deletion is unavailable. For CTC cache file manual deletion, complete the [“Delete the CTC Cache File Manually” procedure on page 1-49](#).

Figure 1-21 Deleting the CTC Cache



Delete the CTC Cache File Manually



Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting the CTC cache might cause any CTC running on this system to behave in an unexpected manner.

- Step 1** To delete the JAR files manually, from the Windows Start menu choose **Search > For Files or Folders**.
- Step 2** Enter *.jar in the Search for files or folders named field in the Search Results dialog box and click **Search Now**.
- Step 3** Click the **Modified** column in the Search Results dialog box to find the JAR files that match the date when you downloaded the files from the TCC2. These files might include CTC*.jar, CMS*.jar, and jar_cache*.tmp.
- Step 4** Highlight the files and press the keyboard **Delete** key.

Step 5 Click **Yes** in the Confirm dialog box.

1.7.7 Node Icon is Gray on CTC Network View

Symptom The CTC network view shows one or more node icons as gray in color and without a node name.

Possible Cause Different CTC releases not recognizing each other.

Recommended Action Correct the core version build as described in the [“Different CTC Releases Do Not Recognize Each Other”](#) section on page 1-52.

Possible Cause A username/password mismatch.

Recommended Action Correct the username and password as described in the [“Username or Password Do Not Match”](#) section on page 1-53.

Possible Cause No IP connectivity between nodes.

Recommended Action Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the [“Ethernet Connections”](#) section on page 1-55.

Possible Cause A lost DCC connection.

Recommended Action Usually accompanied by an embedded operations channel (EOC) alarm. Clear the EOC alarm and verify the DCC connection as described in the [“EOC”](#) alarm.

1.7.8 CTC Cannot Launch Due to Applet Security Restrictions

Symptom The error message “Unable to launch CTC due to applet security restrictions” appears after you enter the IP address in the browser window.

Possible Cause You are logging into a node running CTC Software R4.0 or earlier. Releases earlier than R4.1 require a modification to the java.policy file so that CTC JAR files can be downloaded to the computer. The modified java.policy file might not exist on the computer.

Recommended Action Install the software CD for the release of the node you are logging into. Run the CTC Setup Wizard (double-click **Setup.exe**). Choose **Custom installation**, then choose the Java Policy option. For additional information, refer to the CTC installation information in the *Cisco ONS 15454 Procedure Guide*. If the software CD is not available, you must manually edit the java.policy file on your computer. Complete the [“Manually Edit the java.policy File”](#) procedure on page 1-50.

Manually Edit the java.policy File

Step 1 Search your computer for java.policy file and open it with a text editor (Notepad or Wordpad).

Step 2 Verify that the end of this file has the following lines:

```
// Insert this into the system-wide or a per-user java.policy file.
// DO NOT OVERWRITE THE SYSTEM-WIDE POLICY FILE--ADD THESE LINES!

grant codeBase "http://*/fs/LAUNCHER.jar {
permission java.security.AllPermission;
};
```

Step 3 If these five lines are not in the file, enter them manually.

Step 4 Save the file and restart Netscape.

CTC should now start correctly.

Step 5 If the error message is still reported, save the java.policy file as **.java.policy**. On Win98/2000 PCs, save the file to the C:\Windows folder. On Windows NT 4.0 or later PCs, save the file to all of the user folders on that PC, for example, C:\Winnt\profiles\joeuser.

1.7.9 Java Runtime Environment Incompatible

Symptom The CTC application does not run properly.

Possible Cause The compatible Java 2 JRE is not installed.

Recommended Action The JRE contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language. The ONS 15454 CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD and on the Cisco ONS 15454 documentation CD. Complete the [“Launch CTC to Correct the Core Version Build” procedure on page 1-52](#). If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. [Table 1-3](#) shows JRE compatibility with ONS 15454 software releases.

Table 1-3 JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15454 R2.2.1 and earlier	Yes	No	No
ONS 15454 R2.2.2	Yes	Yes	No
ONS 15454 R3.0	Yes	Yes	No
ONS 15454 R3.1	Yes	Yes	No
ONS 15454 R3.2	Yes	Yes	No
ONS 15454 R3.3	Yes	Yes	No
ONS 15454 R3.4	No	Yes	No
ONS 15454 R4.0 ¹	No	Yes	No
ONS 15454 R4.1	No	Yes	No
ONS 15454 R4.5	No	Yes	No

Table 1-3 JRE Compatibility (continued)

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15454 R4.6	No	Yes	Yes
ONS 15454 R4.7	No	No	Yes

1. Software R4.0 notifies you if an earlier JRE version is running on your PC or UNIX workstation.

Launch CTC to Correct the Core Version Build

-
- Step 1** Exit the current CTC session and completely close the browser.
- Step 2** Start the browser.
- Step 3** Type the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged in with or an IP address other than the original.
- Step 4** Log into CTC. The browser downloads the JAR file from CTC.



Note

After R2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to the ONS 15454, ONS 15454 SDH, and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 R1.0 uses a 2.3 core build and a 1.0 element build. To display the CTC Core Version number, from the CTC menu bar click **Help > About CTC**. This lists the core and element builds discovered on the network.

1.7.10 Different CTC Releases Do Not Recognize Each Other

Symptom This situation is often accompanied by the INCOMPATIBLE-SW alarm.

Possible Cause The software loaded on the connecting workstation and the software on the TCC2 card are incompatible.

Recommended Action This occurs when the TCC2 software is upgraded but the PC has not yet upgraded the compatible CTC JAR file. It also occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version. Complete the [“Launch CTC to Correct the Core Version Build” procedure on page 1-52](#).



Note

Remember to always log into the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 2.2 or lower and then attempt to log into another ONS node in the network running a higher CTC core version, the lower version node does not recognize the new node.

Launch CTC to Correct the Core Version Build

-
- Step 1** Exit the current CTC session and completely close the browser.

- Step 2** Start the browser.
- Step 3** Type the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.
- Step 4** Log into CTC. The browser downloads the JAR file from CTC.



Note After R2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to the ONS 15454, ONS 15454 SDH, and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 R1.0 uses a 2.3 core build and a 1.0 element build. To display the CTC Core Version number, from the CTC menu bar click **Help > About CTC**. This lists the core and element builds discovered on the network.

1.7.11 Username or Password Do Not Match

Symptom A mismatch often occurs concurrently with a NOT-AUTHENTICATED alarm.

Possible Cause The username or password entered does not match the information stored in the TCC2.

Recommended Action All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes. For initial login to the ONS 15454, type the CISCO15 user name in capital letters and click **Login** (no password is required). If you are using a CTC Software R2.2.2 or earlier and CISCO15 does not work, type cerent454 for the user name. Complete the [“Verify Correct Username and Password” procedure on page 1-53](#).

Verify Correct Username and Password

-
- Step 1** Ensure that your keyboard Caps Lock key is not turned on and affecting the case-sensitive entry of the username and password.
- Step 2** Contact your system administrator to verify the username and password.
- Step 3** Call Cisco Technical Support (1 800 553-2447) to have them enter your system and create a new user name and password.
-

1.7.12 No IP Connectivity Exists Between Nodes

Symptom The nodes have a gray icon and is usually accompanied by alarms.

Possible Cause A lost Ethernet connection.

Recommended Action Usually is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the “[Ethernet Connections](#)” section on page 1-55.

1.7.13 DCC Connection Lost

Symptom The node is usually accompanied by alarms and the nodes in the network view have a gray icon. This symptom is usually accompanied by an EOC alarm.

Possible Cause A lost DCC connection.

Recommended Action Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the “[EOC](#)” alarm.

1.7.14 “Path in Use” Error When Creating a Circuit

Symptom While creating a circuit, you get a “Path in Use” error that prevents you from completing the circuit creation.

Possible Cause Another user has already selected the same source port to create another circuit.

Recommended Action CTC does not remove a card or port from the available list until a circuit is completely provisioned. If two users simultaneously select the same source port to create a circuit, the first user to complete circuit provisioning gets use of the port. The other user gets the “Path in Use” error. Cancel the circuit creation and start over, or click **Back** until you return to the initial circuit creation window. The source port that was previously selected no longer appears in the available list because it is now part of a provisioned circuit. Select a different available port and begin the circuit creation process again.

1.7.15 Calculate and Design IP Subnets

Symptom You cannot calculate or design IP subnets on the ONS 15454.

Possible Cause The IP capabilities of the ONS 15454 require specific calculations to properly design IP subnets.

Recommended Action Cisco provides a free online tool to calculate and design IP subnets. Go to http://www.cisco.com/techtools/ip_addr.html. For information about ONS 15454 IP capability, refer to the *Cisco ONS 15454 Reference Manual*.

1.7.16 Ethernet Connections

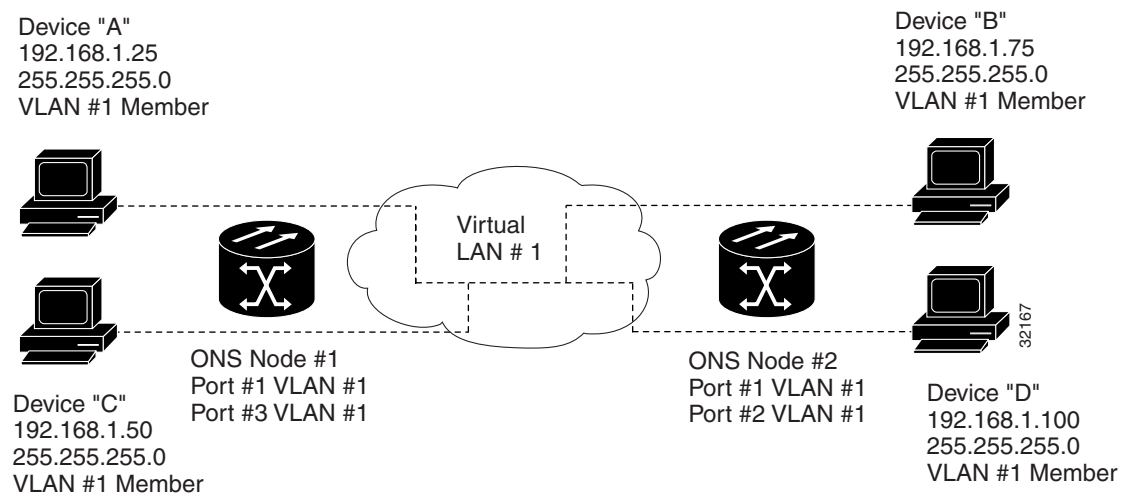
Symptom Ethernet connections appear to be broken or are not working properly.

Possible Cause Improperly seated connections.

Possible Cause Incorrect connections.

Recommended Action You can fix most connectivity problems in an Ethernet network by following a few guidelines. See [Figure 1-22](#) when using the steps in the “[Verify Ethernet Connections](#)” procedure on page 1-55.

Figure 1-22 Ethernet Connectivity Reference



Verify Ethernet Connections

- Step 1** Verify that the alarm filter is turned OFF.
- Step 2** Check for SONET and dense wavelength division multiplexing (DWDM) alarms on the STS that carries the VLAN Ethernet circuit. Clear any alarms by looking them up in [Chapter 2, “Alarm Troubleshooting.”](#)
- Step 3** Check for Ethernet-specific alarms. Clear any raised alarms by looking up that alarm in [Chapter 2, “Alarm Troubleshooting.”](#)
- Step 4** Verify that the ACT LED on the Ethernet card is green.
- Step 5** Verify that Ports 1 and 3 on ONS 15454 #1 and Ports 1 and 2 on ONS 15454 #2 have green link-integrity LEDs illuminated.
- Step 6** If no green link-integrity LED is illuminated for any of these ports:
 - a. Verify physical connectivity between the ONS 15454s and the attached device.
 - b. Verify that the ports are enabled on the Ethernet cards.
 - c. Verify that you are using the proper Ethernet cable and that it is wired correctly, or replace the cable with a known-good Ethernet cable.

- d. Check the status LED on the Ethernet card faceplate to ensure the card booted up properly. This LED should be steady green. If necessary, remove and reinsert the card and allow it to reboot.
 - e. It is possible that the Ethernet port is functioning properly but the link LED itself is broken. Complete the [“Verify General Card LED Operation” procedure on page 1-28](#).
- Step 7** Verify connectivity between device A and device C by pinging between these locally attached devices. Complete the [“Verify PC Connection to the ONS 15454 \(ping\)” procedure on page 1-43](#). If the ping is unsuccessful:
- a. Verify that device A and device C are on the same IP subnet.
 - b. open the Ethernet card in CTC card view and click the **Provisioning > VLAN** tab to verify that both Port 1 and Port 3 on the card are assigned to the same VLAN.
 - c. If a port is not assigned to the correct VLAN, click that port column in the VLAN row and set the port to Tagged or Untag. Click **Apply**.
- Step 8** Repeat [Step 7](#) for devices B and D.
- Step 9** Verify that the Ethernet circuit that carries VLAN #1 is provisioned and that ONS 15454 #1 and ONS 15454 #2 ports also use VLAN #1.
-

1.7.17 VLAN Cannot Connect to Network Device from Untag Port

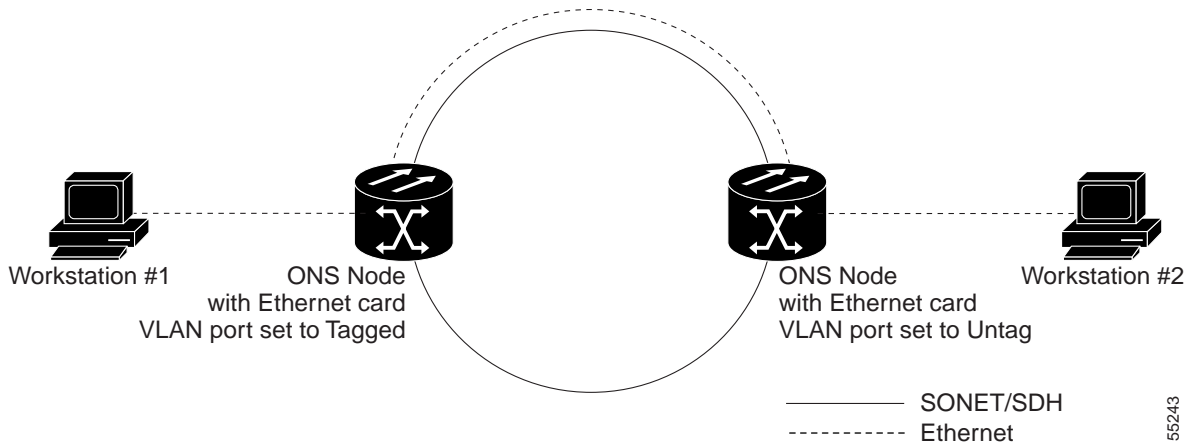
Symptom Networks that have a VLAN with one ONS 15454 Ethernet card port set to Tagged and one ONS 15454 Ethernet card set to Untag might have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port ([Figure 1-23](#)). They might also see a higher than normal runt packets count at the network device attached to the Untag port. This symptom/limitation also exists when ports within the same card or ports within the same chassis are put on the same VLAN, with a mix of tagged and untagged.

Possible Cause The Tagged ONS 15454 adds the IEEE 802.1Q tag and the Untag ONS 15454 removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet.

Possible Cause Dropped packets can also occur when ARP attempts to match the IP address of the network device attached to the Untag port with the physical MAC address required by the network access layer.

Recommended Action The solution is to set both ports in the VLAN to Tagged to stop the stripping of the 4 bytes from the data packet and prevent the NIC card in the network access device from recognizing the packet as a runt and dropping it. Network devices with IEEE 802.1Q-compliant NIC cards accept the tagged packets. Network devices with non IEEE 802.1Q compliant NIC cards still drop these tagged packets. The solution might require upgrading network devices with non-IEEE 802.1Q compliant NIC cards to IEEE 802.1Q compliant NIC cards. You can also set both ports in the VLAN to Untag, but you will lose IEEE 802.1Q compliance.

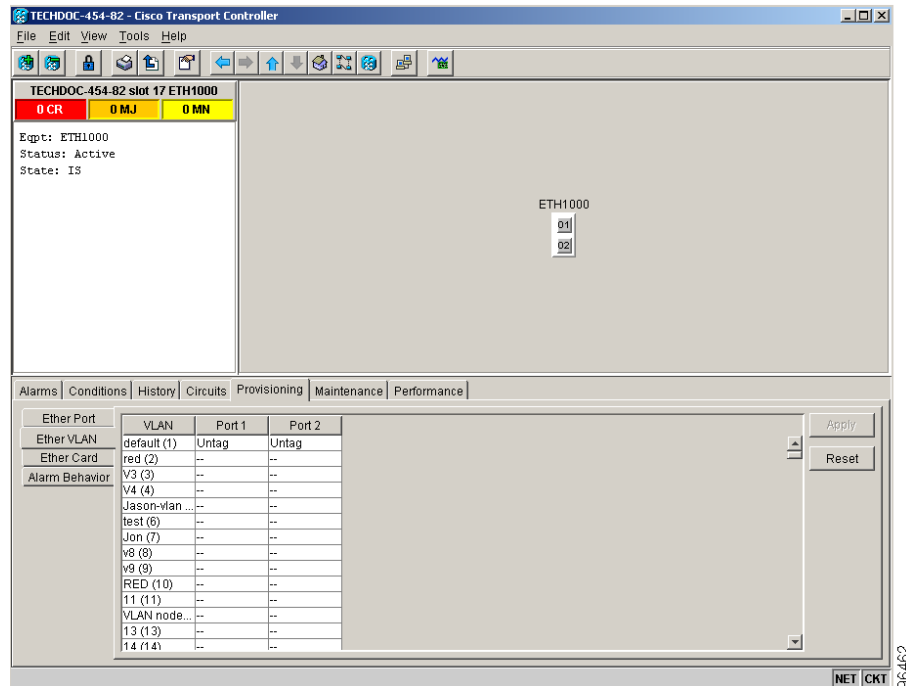
Figure 1-23 VLAN with Ethernet Ports at Tagged and Untag



Change VLAN Port Tag and Untag Settings

- Step 1 Display the CTC card view for the Ethernet card involved in the problem VLAN.
- Step 2 Click the **Provisioning > Ether VLAN** tab (Figure 1-24).

Figure 1-24 Configuring VLAN Membership for Individual Ethernet Ports



- Step 3 If the port is set to **Tagged**, continue to look at other cards and their ports in the VLAN until you find the port that is set to **Untag**.
- Step 4 At the VLAN port set to **Untag**, click the port and choose **Tagged**.



Note The attached external devices must recognize IEEE 802.1Q VLANs.

Step 5 After each port is in the appropriate VLAN, click **Apply**.

1.8 Circuits and Timing

This section provides solutions to circuit creation and reporting errors, as well as common timing reference errors and alarms.

1.8.1 OC-N Circuit Transitions to Partial State

Symptom An automatic or manual transition of a circuit from one state to another state results in the OOS-PARTIAL status, which indicates that not all OC-N connections in the circuit are in the IS-NR service state.

Possible Cause During a manual transition, CTC cannot communicate with one of the nodes or one of the nodes is on a version of software that does not support the new state model.

Recommended Action Repeat the manual transition operation. If the partial state persists, determine which node in the circuit is not changing to the desired state. Complete the [“View the State of OC-N Circuit Nodes” procedure on page 1-58](#). Log into the circuit node that did not change to the desired state and determine the version of software. If the software on the node is Software R3.3 or earlier, upgrade the software. Refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures.



Note If the node software cannot be upgraded to R4.0, the partial state condition can be avoided by using only the circuit state supported in the earlier software version.

Possible Cause During an automatic transition, some path-level defects and/or alarms were detected on the circuit.

Possible Cause One end of the circuit is not properly terminated.

Recommended Action Determine which node in the circuit is not changing to the desired state. Complete the [“View the State of OC-N Circuit Nodes” procedure on page 1-58](#). Log onto the circuit node that did not change to the desired state and examine the circuit for path-level defects, improper circuit termination, or alarms. Refer to the *Cisco ONS 15454 Procedure Guide* for procedures to clear alarms and change circuit configuration settings. Resolve and clear the defects and/or alarms on the circuit node and verify that the circuit transitions to the desired state.

View the State of OC-N Circuit Nodes

Step 1 Click the **Circuits** tab.

- Step 2** From the Circuits tab list, select the circuit with the *_PARTIAL status condition.
- Step 3** Click **Edit**. The Edit Circuit window appears.
- Step 4** In the Edit Circuit window, click the **State** tab (if you are viewing a SONET circuit).
The State tab window lists the Node, End A, End B, CRS admin state, and CRS Service State for each of the nodes in the circuit.
-

1.8.2 AIS-V on DS3XM-6 Unused VT Circuits

Symptom An incomplete circuit path causes an AIS.

Possible Cause The port on the reporting node is in-service but a node upstream on the circuit does not have an OC-N port in service.

Recommended Action An AIS-V indicates that an upstream failure occurred at the virtual tributary (VT) layer. AIS-V alarms also occur on DS3XM-6 VT circuits that are not carrying traffic and on stranded bandwidth. Complete the [“Clear AIS-V on DS3XM-6 or DS3XM12 Unused VT Circuits” procedure on page 1-59](#).

Clear AIS-V on DS3XM-6 or DS3XM12 Unused VT Circuits

- Step 1** Determine the affected port.
- Step 2** Record the node ID, slot number, port number, or VT number.
- Step 3** Create a unidirectional VT circuit from the affected port back to itself, such as Source node/Slot 2/Port 2/VT 13 cross connected to Source node/Slot 2/Port 2/VT 13.
- Step 4** Uncheck the **Bidirectional** check box in the circuit creation window.
- Step 5** Give the unidirectional VT circuit an easily recognizable name, such as “delete me.”
- Step 6** Display the DS3XM-6 card in CTC card view. Click the **Maintenance > DS1** tab.
- Step 7** Locate the VT that is reporting the alarm (for example, DS3 #2, DS1 #13).
- Step 8** From the Loopback Type list, choose **Facility (Line)** and click **Apply**.
- Step 9** Click **Circuits**.
- Step 10** Find the one-way circuit you created in [Step 3](#). Select the circuit and click **Delete**. Do not check any check boxes.
- Step 11** Click **Yes** in the Delete Confirmation dialog box.
- Step 12** Display the DS3XM-6 or DS3XM12 card in CTC card view. Click **Maintenance > DS1**.
- Step 13** Locate the VT in Facility (line) Loopback.
- Step 14** From the Loopback Type list, choose **None** and then click **Apply**.
- Step 15** Click the **Alarms** tab and verify that the AIS-V alarms have cleared.
- Step 16** Repeat this procedure for all the AIS-V alarms on the DS3XM-6 or DS3XM12 cards.
-

1.8.3 Circuit Creation Error with VT1.5 Circuit

Symptom You receive an “Error while finishing circuit creation. Unable to provision circuit. Unable to create connection object at *node_name*” message when trying to create a VT1.5 circuit in CTC.

Possible Cause You might have run out of bandwidth on the VT cross-connect matrix at the ONS 15454 indicated in the error message.

Recommended Action The matrix has a maximum capacity of 336 bidirectional VT1.5 cross-connects. Certain configurations exhaust VT capacity with less than 336 bidirectional VT1.5s in a BLSR or less than 224 bidirectional VT1.5s in a path protection or 1+1 protection group. Refer to the *Cisco ONS 15454 Reference Manual* for more information.

1.8.4 Unable to Create Circuit From DS-3 Card to DS3XM-6 or DS3XM12 Card

Symptom You cannot create a circuit from a DS-3 card to a DS3XM-6 or DS3XM12 card.

Possible Cause A DS-3 card and a DS3XM-6 or DS3XM12 card have different functions.

Recommended Action A DS3XM-6 card converts each of its six DS-3 interfaces into 28 DS-1s for cross-connection through the network. The DS3XM12 converts each of its 12 interfaces into up to 48 DS-1s. Thus, you can create a circuit from a DS3XM-6 or DS3XM12 card to a DS-1 card, but not from a DS3XM card to a DS-3 card. These differences are evident in the STS path overhead. The DS-3 card uses asynchronous mapping for DS-3, which is indicated by the C2 byte in the STS path overhead that has a hex code of 04. A DS3XM-6 or DS3XM12 has a VT payload with a C2 hex value of 02.



Note You can find instructions for creating circuits in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

1.8.5 DS-3 Card Does Not Report AIS-P From External Equipment

Symptom A DS3-12, DS3N-12, DS3-12E, or DS3N-12E card does not report STS AIS-P from the external equipment/line side.

Possible Cause The card is functioning as designed.

Recommended Action This card terminates the port signal at the backplane so STS AIS-P is not reported from the external equipment/line side. DS3-12, DS3N-12, DS3-12E, and DS3N-12E cards have DS3 header monitoring functionality, which allows you to view performance monitoring (PM) on the DS3 path. Nevertheless, you cannot view AIS-P on the STS path. For more information about the PM capabilities of the DS3-12, DS3N-12, DS3-12E or DS3N-12E cards, refer to the *Cisco ONS 15454 Reference Manual*.

1.8.6 OC-3 and DCC Limitations

Symptom Limitations to OC-3 and DCC usage.

Possible Cause OC-3 and DCC have limitations for the ONS 15454.

Recommended Action For an explanation of OC-3 and DCC limitations, refer to the DCC Tunnels section of the *Cisco ONS 15454 Procedure Guide*.

1.8.7 ONS 15454 Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

Possible Cause The optical or BITS input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source.

Possible Cause The optical or building integrated timing supply (BITS) input is not functioning.

Possible Cause The synchronization status messaging (SSM) message is set to do not use for synchronization (DUS).

Possible Cause SSM indicates a Stratum 3 or lower clock quality.

Possible Cause The input frequency is off by more than 15 ppm.

Possible Cause The input clock wanders and has more than three slips in 30 seconds.

Possible Cause A bad timing reference existed for at least two minutes.

Recommended Action The ONS 15454 internal clock operates at a Stratum 3E level of accuracy. This gives the ONS 15454 a free-running synchronization accuracy of ± 4.6 ppm and a holdover stability of less than 255 slips in the first 24 hours or 3.7×10^{-7} /day, including temperature. ONS 15454 free-running synchronization relies on the Stratum 3 internal clock. Over an extended time period, using a higher quality Stratum 1 or Stratum 2 timing source results in fewer timing slips than a lower quality Stratum 3 timing source.

1.8.8 Holdover Synchronization Alarm

Symptom The clock is running at a different frequency than normal and the “[HLDVRSYNC](#)” alarm appears.

Possible Cause The last reference input has failed.

Recommended Action The clock is running at the frequency of the last known-good reference input. This alarm is raised when the last reference input fails. See the “[HLDVRSYNC](#)” section on [page 2-116](#) for a detailed description of this alarm.



Note The ONS 15454 supports holdover timing per Telcordia GR-436 when provisioned for external (BITS) timing.

1.8.9 Free-Running Synchronization Mode

Symptom The clock is running at a different frequency than normal and the “FRNGSYNC” alarm appears.

Possible Cause No reliable reference input is available.

Recommended Action The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the “FRNGSYNC” condition on page 2-103 for a detailed description.

1.8.10 Daisy-Chaind BITS Not Functioning

Symptom You are unable to daisy chain the BITS sources.

Possible Cause Daisy-chained BITS sources are not supported on the ONS 15454.

Recommended Action Daisy-chained BITS sources cause additional wander buildup in the network and are therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each ONS 15454.

1.8.11 Blinking STAT LED after Installing a Card

Symptom After installing a card, the STAT LED blinks continuously for more than 60 seconds.

Possible Cause The card cannot boot because it failed the Power On Shelf Test (POST) diagnostics.

Recommended Action The blinking STAT LED indicates that POST diagnostics are being performed. If the LED continues to blink more than 60 seconds, the card has failed the POST diagnostics test and has failed to boot. If the card has truly failed, an “EQPT” alarm is raised against the slot number with an “Equipment Failure” description. Check the alarm tab for this alarm to appear for the slot where the card was installed. To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card. Complete the “Air Filter and Fan Procedures” procedure on page 2-257.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the “Protection Switching, Lock Initiation, and Clearing” section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

1.9 Fiber and Cabling

This section explains problems typically caused by cabling connectivity errors. It also includes instructions for crimping CAT-5 cable and lists the optical fiber connectivity levels.

1.9.1 Bit Errors Appear for a Traffic Card

Symptom A traffic card has multiple bit errors.

Possible Cause Faulty cabling or low optical-line levels.

Recommended Action Bit errors on line (traffic) cards usually originate from cabling problems or low optical-line levels. The errors can be caused by synchronization problems, especially if PJ (pointer justification) errors are reported. Moving cards into different error-free slots will isolate the cause. Use a test set whenever possible because the cause of the errors could be external cabling, fiber, or external equipment connecting to the ONS 15454. Troubleshoot cabling problems using the [“Troubleshooting Non-DWDM Circuit Paths with Loopbacks”](#) section on page 1-2. Troubleshoot low optical levels using the [“Faulty Fiber-Optic Connections”](#) section on page 1-63.

1.9.2 Faulty Fiber-Optic Connections

Symptom A line card has multiple SONET/DWDM alarms and/or signal errors.

Possible Cause Faulty fiber-optic connections.

Recommended Action Faulty fiber-optic connections can be the source of SONET/DWDM alarms and signal errors. Complete the [“Verify Fiber-Optic Connections”](#) procedure on page 1-64.

Possible Cause Faulty CAT-5 cables.

Recommended Action Faulty CAT-5 cables can be the source of SONET/DWDM alarms and signal errors. Complete the [“Crimp Replacement LAN Cables”](#) section on page 1-65.

Possible Cause Faulty Gigabit Interface Converters (GBIC).

Recommended Action Faulty GBICs can be the source of SONET/DWDM alarms and signal errors. See the [“Replace Faulty GBIC or SFP Connectors”](#) section on page 1-67.



Follow all directions and warning labels when working with optical fibers. To prevent eye damage, never look directly into a fiber or connector. Class IIIb laser. Danger, laser radiation when open. The OC-192 laser is off when the safety key is off (labeled 0). The laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. Avoid direct exposure to the beam. Invisible radiation is emitted from the aperture at the end of the fiber optic cable when connected, but not terminated.

Verify Fiber-Optic Connections

Step 1 Ensure that a single-mode fiber connects to the ONS 15454 OC-N card.



Note SM or SM Fiber should be printed on the fiber span cable. ONS 15454 OC-N cards do not use multimode fiber.

Step 2 Ensure that the connector keys on the SC fiber connector are properly aligned and locked.

Step 3 Check that the single-mode fiber power level is within the specified range:

- a. Remove the Rx end of the suspect fiber.
- b. Connect the receive end of the suspect fiber to a fiber-optic power meter, such as a GN Nettest LP-5000.
- c. Determine the power level of fiber with the fiber-optic power meter.
- d. Verify the power meter is set to the appropriate wavelength for the OC-N card being tested (either 1310 nm or 1550 nm depending on the specific card).
- e. Verify that the power level falls within the range specified for the card if it is an OC-N card; see the [“OC-N Card Transmit and Receive Levels”](#) section on page 1-71.

Step 4 If the power level falls below the specified range for the OC-N card:

- a. Clean or replace the fiber patch cords. Clean the fiber according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. If possible, do this for the OC-N card you are working on and the far-end card.
- b. Clean the optical connectors on the card. Clean the connectors according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. If possible, do this for the OC-N card you are working on and the far-end card.
- c. Ensure that the far-end transmitting card is not an ONS intermediate-range (IR) card when an ONS long-range (LR) card is appropriate.
IR cards transmit a lower output power than LR cards.
- d. Replace the far-end transmitting OC-N card to eliminate the possibility of a degrading transmitter on this OC-N card.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the [“Protection Switching, Lock Initiation, and Clearing”](#) section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

- e. If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):
 - Excessive fiber distance; single-mode fiber attenuates at approximately 0.5 dB/km.
 - Excessive number or fiber connectors; connectors take approximately 0.5 dB each.
 - Excessive number of fiber splices; splices take approximately 0.5 dB each.

**Note**

These are typical attenuation values. Refer to the specific product documentation for the actual values or use an optical time domain reflectometer (OTDR) to establish precise link loss and budget requirements.

- Step 5** If no power level shows on the fiber, the fiber is bad or the transmitter on the OC-N card failed.
- Check that the Tx and Rx fibers are not reversed. LOS and EOC alarms normally accompany reversed Tx and Rx fibers. Switching reversed Tx and Rx fibers clears the alarms and restores the signal.
 - Clean or replace the fiber patch cords. Clean the fiber according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. If possible, do this for the OC-N card you are working on and the far-end card.
 - Retest the fiber power level.
 - If the replacement fiber still shows no power, replace the OC-N card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the [“Protection Switching, Lock Initiation, and Clearing”](#) section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

- Step 6** If the power level on the fiber is above the range specified for the card, ensure that an ONS LR card is not being used when an ONS IR card is appropriate.

LR cards transmit a higher output power than IR cards. When used with short runs of fiber, an LR transmitter will be too powerful for the receiver on the receiving OC-N card.

Receiver overloads occur when maximum receiver power is exceeded.

**Tip**

To prevent overloading the receiver, use an attenuator on the fiber between the ONS OC-N card transmitter and the receiver. Place the attenuator on the receive transmitter of the ONS OC-N cards. Refer to the attenuator documentation for specific instructions.

**Tip**

Most fiber has text printed on only one of the two fiber strands. Use this to identify which fiber is connected to Tx and which fiber is connected to Rx.

1.9.2.1 Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the ONS 15454. Use a cross-over cable when connecting an ONS 15454 to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15454 to a router or workstation. Use CAT-5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. [Figure 1-25](#) shows the wiring of an RJ-45 connector. [Figure 1-26](#) shows a LAN cable layout, and [Table 1-4](#) shows the cable pinouts. [Figure 1-27](#) shows a cross-over cable layout, and [Table 1-5](#) shows the cross-over pinouts.

Figure 1-25 RJ-45 Pin Numbers

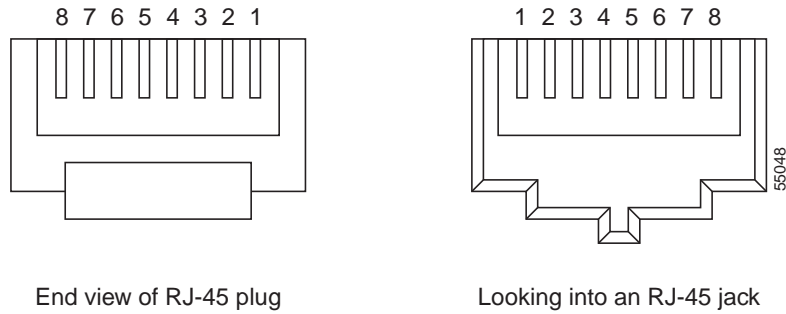


Figure 1-26 LAN Cable Layout

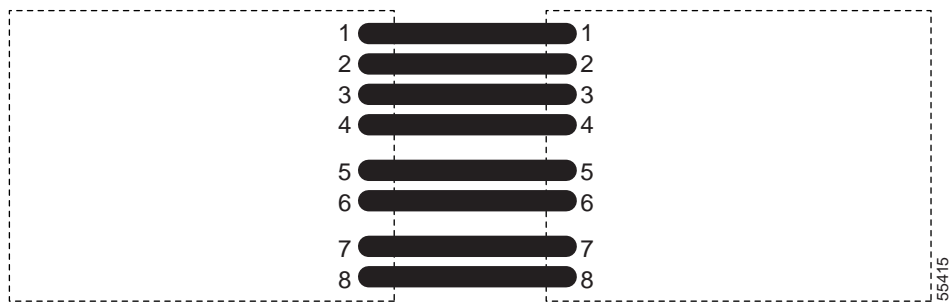


Table 1-4 LAN Cable Pinout

Pin	Color	Pair	Name	Pin
1	white/orange	2	Transmit Data +	1
2	orange	2	Transmit Data —	2
3	white/green	3	Receive Data +	3
4	blue	1	—	4
5	white/blue	1	—	5
6	green	3	Receive Data —	6
7	white/brown	4	—	7
8	brown	4	—	8

Figure 1-27 Cross-Over Cable Layout

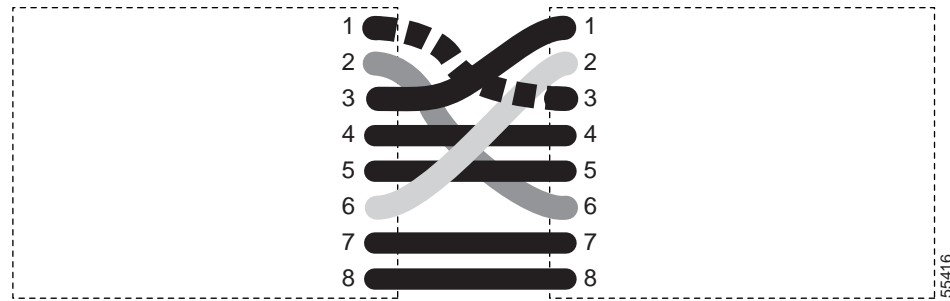


Table 1-5 Cross-Over Cable Pinout

Pin	Color	Pair	Name	Pin
1	white/orange	2	Transmit Data +	3
2	orange	2	Transmit Data —	6
3	white/green	3	Receive Data +	1
4	blue	1	—	4
5	white/blue	1	—	5
6	green	3	Receive Data —	2
7	white/brown	4	—	7
8	brown	4	—	8

**Note**

Odd-numbered pins always connect to a white wire with a colored stripe.

1.9.2.2 Replace Faulty GBIC or SFP Connectors

GBICs and small form-factor pluggables (SFP) are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

**Warning**

GBICs are Class I laser products. These products have been tested and comply with Class I limits.

**Warning**

Invisible laser radiation might be emitted from the aperture ports of the single-mode fiber optic modules when no cable is connected. Avoid exposure and do not stare into open apertures.

GBICs and SFPs are input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. The type of GBIC or SFP determines the maximum distance that the Ethernet traffic can travel from the card to the next network device. For a description of GBICs and SFPs and their capabilities, see [Table 1-6](#) and [Table 1-7 on page 1-68](#), and refer to the *Cisco ONS 15454 Reference Manual*.

**Note**

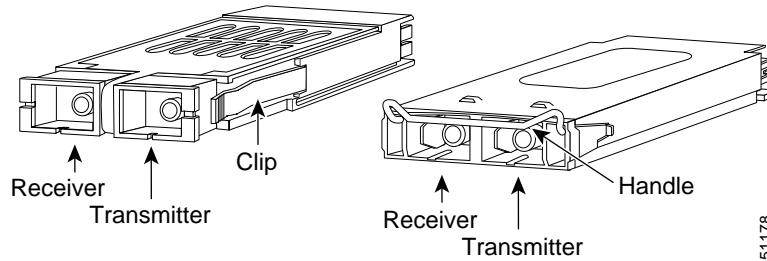
GBICs and SFPs must be matched on either end by type: SX to SX, LX to LX, or ZX to ZX.

**Note**

DWDM and coarse wavelength division multiplexing (CWDM) GBICs do not function with Software R4.7.

GBICs are available in two different models. One GBIC model has two clips (one on each side of the GBIC) that secure the GBIC in the slot on the E1000-2-G, G-Series, or G1K-4 card. The other model has a locking handle. Both models are shown in [Figure 1-28](#).

Figure 1-28 GBICs



[Table 1-6](#) shows the available GBICs. [Table 1-7](#) shows the available SFPs.

**Note**

GBICs are very similar in appearance. Check the GBIC label carefully before installing it.

Table 1-6 Available GBICs

GBIC	Associated Cards	Application	Fiber	Product Number
1000BaseSX	E1000-2-G G-Series G1K-4	Short reach	Multimode fiber up to 550 m long	15454E-GBIC-SX=
1000BaseLX	E1000-2-G G-Series G1K-4	Long reach	Single-mode fiber up to 10 km long	15454E-GBIC-LX=
1000BaseZX	G-Series G1K-4	Extra long reach	Single-mode fiber up to 70 km long	15454E-GBIC-ZX=

Table 1-7 Available SFPs

SFP	Associated Cards	Application	Fiber	Product Number
1000BaseSX	ML1000-2	Short reach	Multimode fiber up to 550 m long	15454E-SFP-LC-SX=
1000BaseLX	ML1000-2	Long reach	Single-mode fiber up to 10 km long	15454E-SFP-LC-LX=

Remove GBIC or SFP Connectors

- Step 1** Disconnect the network fiber cable from the GBIC SC connector or SFP LC duplex connector.

**Warning**

Invisible laser radiation might be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

- Step 2** Release the GBIC or SFP from the slot by simultaneously squeezing the two plastic tab on each side.
- Step 3** Slide the GBIC or SFP out of the Gigabit Ethernet module slot. A flap closes over the GBIC or SFP slot to protect the connector on the Gigabit Ethernet card.
-

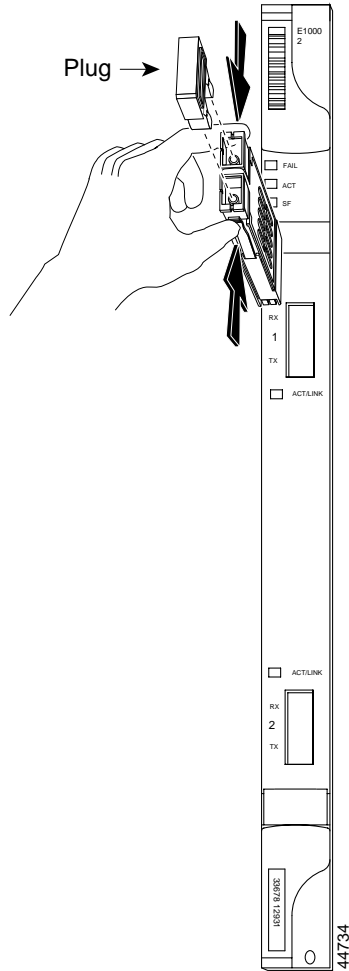
Installing a GBIC with Clips

-
- Step 1** Remove the GBIC from its protective packaging.
- Step 2** Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.
- Step 3** Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.
- Step 4** Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, or G-Series card ([Figure 1-29](#)).

**Note**

GBICs are keyed to prevent incorrect installation.

Figure 1-29 GBIC Installation (with Clips)



- Step 5** Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.
- Step 6** When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.
- Step 7** Return to your originating procedure (NTP).

Installing a GBIC with a Handle

- Step 1** Remove the GBIC from its protective packaging.
- Step 2** Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.
- Step 3** Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.
- Step 4** Remove the protective plug from the SC-type connector.
- Step 5** Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, G1K-4, or G-Series card.



Note GBICs are keyed to prevent incorrect installation.

- Step 6** Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to SC-type connector.
- Step 7** Return to your originating procedure (NTP).

1.9.3 OC-N Card Transmit and Receive Levels

Each OC-N card has a transmit and receive connector on its faceplate. [Table 1-8](#) lists these levels.

Table 1-8 OC-N Card Transmit and Receive Levels

OC-N Card	Receive	Transmit
OC3 IR4/STM1SH 1310	-28 to -8 dBm	-15 to -8 dBm
OC3 IR/STM 1SH 1310-8	-30 to -8 dBm	-15 to -8 dBm
OC12 IR/STM4 SH 1310	-28 to -8 dBm	-15 to -8 dBm
OC12 LR/STM4 LH 1310	-28 to -8 dBm	-3 to +2 dBm
OC12 LR/STM4 LH 1550	-28 to -8 dBm	-3 to +2 dBm
OC12 IR/STM4 SH 1310-4	-28 to -8 dBm	-3 to +2 dBm
OC48 IR/STM16 SH AS 1310	-18 to 0 dBm	-5 to 0 dBm
OC48 LR/STM16 LH AS 1550	-28 to -8 dBm	-2 to +3 dBm
OC48 ELR/STM16 EH 100GHz	-28 to -8 dBm	-2 to 0 dBm
OC192 SR/STM64 IO 1310	-11 to -1 dBm	-6 to -1 dBm
OC192 IR STM64 SH 1550	-14 to -1 dBm	-1 to +2 dBm
OC192 LR/STM64 LH 1550	-21 to -9 dBm	+7 to +10 dBm
OC192 LR/STM64 LH ITU 15xx.xx	-22 to -9 dBm	+3 to +6 dBm
TXP-MR-10G		
Trunk side:	-26 to -8 dBm	-16 to +3 dBm
Client side:	-14 to -1 dBm	-6 to -1 dBm
MXP-2.5G-10G		
Trunk side:	-26 to -8 dBm	-16 to +3 dBm
Client side:	depends on SFP	depends on SFP

1.10 Power Supply Problems

Symptom Loss of power or low voltage, resulting in a loss of traffic and causing the LCD clock to reset to the default date and time.

Possible Cause Loss of power or low voltage.

Possible Cause Improperly connected power supply.

Recommended Action The ONS 15454 requires a constant source of DC power to properly function. Input power is -48 VDC. Power requirements range from -42 VDC to -57 VDC. A newly installed ONS 15454 that is not properly connected to its power supply does not operate. Power problems can be confined to a specific ONS 15454 or affect several pieces of equipment on the site. A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15454 to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning > General > General** tab and change the Date and Time fields. Complete the [“Isolate the Cause of Power Supply Problems”](#) procedure on page 1-72.



Warning

When working with live power, always use proper tools and eye protection.



Warning

Always use the supplied electrostatic discharge (ESD) wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.



Caution

Operations that interrupt power supply or short the power connections to the ONS 15454 are service-affecting.

Isolate the Cause of Power Supply Problems

- Step 1** If a single ONS 15454 show signs of fluctuating power or power loss:
- a. Verify that the -48 VDC #8 power terminals are properly connected to a fuse panel. These power terminals are located on the lower section of the backplane EIA under the clear plastic cover.
 - b. Verify that the power cable is #12 or #14 AWG and in good condition.
 - c. Verify that the power cable connections are properly crimped. Stranded #12 or #14 AWG does not always crimp properly with Staycon type connectors.
 - d. Verify that 20-A fuses are used in the fuse panel.
 - e. Verify that the fuses are not blown.
 - f. Verify that a rack-ground cable attaches to the frame-ground terminal (FGND) on the right side of the ONS 15454 EIA. Connect this cable to the ground terminal according to local site practice.
 - g. Verify that the DC power source has enough capacity to carry the power load.
 - h. If the DC power source is battery-based:

- Check that the output power is high enough. Power requirements range from –42 VDC to –57 VDC.
- Check the age of the batteries. Battery performance decreases with age.
- Check for opens and shorts in batteries, which might affect power output.
- If brownouts occur, the power load and fuses might be too high for the battery plant.

- Step 2** If multiple pieces of site equipment show signs of fluctuating power or power loss:
- a. Check the uninterruptible power supply (UPS) or rectifiers that supply the equipment. Refer to the UPS manufacturer's documentation for specific instructions.
 - b. Check for excessive power drains caused by other equipment, such as generators.
 - c. Check for excessive power demand on backup power systems or batteries when alternate power sources are used.
-

1.10.1 Power Consumption for Node and Cards

Symptom You are unable to power up a node or the cards in a node.

Possible Cause Improper power supply.

Recommended Action Refer to power information in the *Cisco ONS 15454 Reference Guide*.
