General Troubleshooting

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15454 DWDM shelf in ANSI or ETSI platforms. To troubleshoot specific alarms, see Chapter 2, "Alarm Troubleshooting." If you cannot find what you are looking for, contact Cisco Technical Support (1 800 553-2447).

Note In this chapter, "ONS 15454" refers to both ANSI and ETSI versions of the platform unless otherwise noted.

This chapter includes the following sections on network problems:

Note For dense wavelength division multiplexing (DWDM) network acceptance tests, 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:

1.1 Loopback Description

Use loopbacks and hairpin circuits to test newly created circuits before running live traffic or to logically locate the source of a network failure. All ONS 15454 and ONS 15454 SDH TXP and MXP cards allow loopbacks and hairpin test circuits. Other cards do not allow loopbacks, including OPT-BST, OPT-PRE, OSC-CSM, AD-xB-xx.x, and AD-xC-xx.x cards.

To create a loopback on an ANSI or SONET port, the port must be in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state. After you create the loopback, the service state becomes Out-of-Service and Management, Loopback and Maintenance (OOS-MA,LPBK & MT).

To create a loopback on an SDH or ETSI port, the port must be in the Locked, maintenance administrative state and the Locked-Enabled, loopback & maintenance administrative state.

Caution Facility 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 procedures exist in Chapter 2, "Alarm Troubleshooting." For more information about these operations, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

Note In CTC, a facility loopback is sometimes called "facility (line)" loopback, and a terminal loopback is sometimes called a "terminal (inward)" loopback. This is done to indicate the terminating direction of the signal: a facility loopback is sent outward toward the span, whereas a terminal loopback is redirected inward toward its originating port.

1.1.1 Facility Loopbacks

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

1.1.1.1 General Behavior

A facility loopback tests the line interface unit (LIU) of a card, the electrical interface assembly (EIA), 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 a card LIU, connect an optical test set to a trunk or client port and perform a facility loopback. Alternately, use a loopback or hairpin circuit on a card that is farther along the circuit path. For example, Figure 1-1 shows a facility loopback at a trunk port and at a client port on a TXP card.

Figure 1-1   Facility Loopback Path on a Near-End Transponder Card
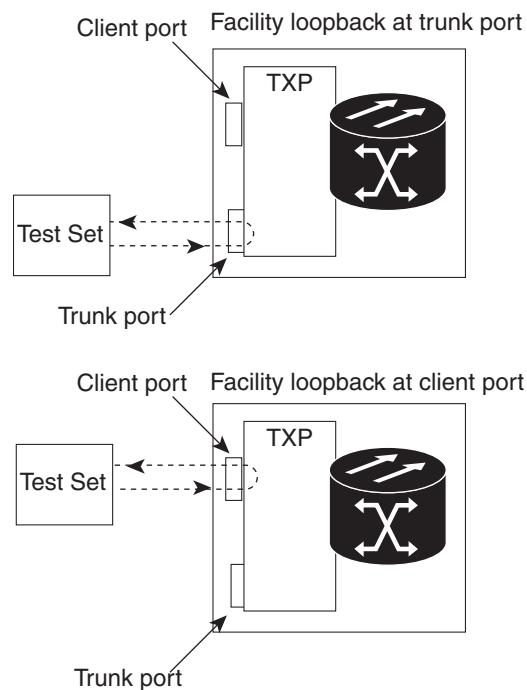
⚠️
Caution   Before performing a facility loopback on a TXP card, be sure that the card contains at least two data communications channel (DCC) paths to the node where the card is installed. A second DCC provides a nonlooped path to log into the node after the loopback is applied, enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the node containing the loopback card.

⚠️
Caution   Ensure that the facility being loopbacked is not being used by the node for line timing. If it is, a timing loop will be created.

1.1.1.2 Card Behavior

Port loopbacks either terminate or bridge the loopback signal. All 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 alarm indication signal (AIS) is injected if the signal is bridged. If the signal is terminated, an applicable AIS is injected downstream.

Table 1-1   DWDM Client Card 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

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

With a client-side SONET or ANSI facility loopback, the client port service state is OOS-MA,LPBK & MT. However any remaining client and trunk ports can be in any other service state. For SONET or ANSI 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.

With a client-side SDH or ESTI facility loopback, the client port is in the Locked-enabled,maintenance & loopback service state, however the remaining client and trunk ports can be in any other service state. For MXP and TXP cards in a SDH or ETSI trunk-side facility loopback, the trunk port is in the Locked-enabled,maintenance & loopback 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 loopback activity.

1.1.2.1 General Behavior

A terminal loopback tests a circuit path as it passes through a TXP or MXP card and loops back. For example, as shown in Figure 1-2, there are two types of terminal loopbacks shown for a TXP card.

The first is a terminal loopback at the client port. In this situation, the test set traffic comes in through the TXP trunk port, travels through the card, and turns around because of the terminal loopback in effect on the card just before it reaches the LIU of the client port. The signal is then sent back through the card to the trunk port and back to the test set.

The second is a terminal loopback at the trunk port. In this situation, the test set traffic comes in through the TXP client port, travels through the card, and turns around because of the terminal loopback in effect on the card just before it reaches the LIU of the trunk port. The signal is then sent back through the card to the client port and back to the test set.

This test verifies that the terminal circuit paths are valid, but does not test the LIU on the TXP card.

Figure 1-2   Terminal Loopback on a TXP Card
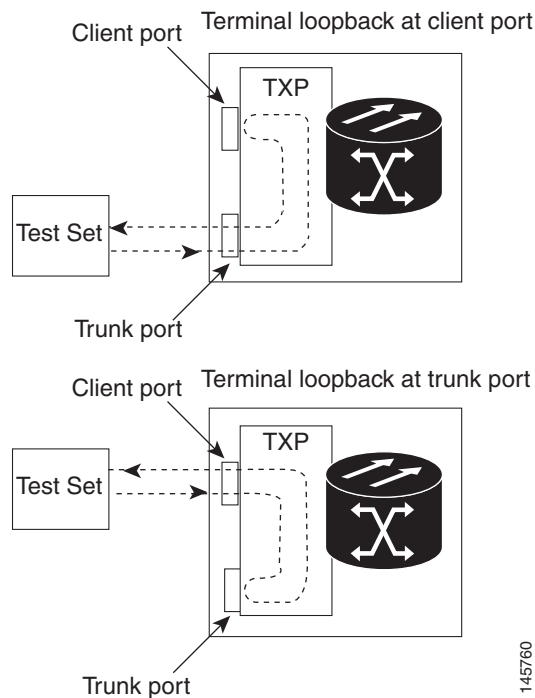
1.1.2.2 Card Behavior

ONS 15454 and ONS 15454 SDH terminal port loopbacks can either terminate or bridge the signal. TXP terminal loopbacks are terminated as shown in Table 1-2. During terminal loopbacks, 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. Client 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.

Table 1-2   Client Card Terminal Loopback Behavior

Card/Port	Terminal Loopback Signal
MXP, MXPP trunk ports	Bridged
MXP, MXPP client ports	Terminated
TXP, MXPP trunk ports	Bridged
TXP, MXPP client ports	Terminated

The MXP and TXP trunk and client ports can simultaneously maintain different service states.

- For SONET or ANSI 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 SONET or ANSI 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 SONET or ANSI 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 service state for complete loopback functionality. A terminal loopback affects all client ports because it is performed on the aggregate signal.

- For SDH or ETSI TXP and TXPP client-side facility loopbacks, the client port is in the Locked-enabled,maintenance & loopback service state and the trunk port must be in Unlocked-enabled service state.

- For SDH or ETSI MXP and MXPP cards with a client-side terminal loopback the client port is in the Locked-enabled,maintenance & loopback service state and remaining client and trunk ports can be in any service state.

- In SDH and ETSI MXP or TXP trunk-side terminal loopbacks, the trunk port is in the Locked-enabled,maintenance & loopback service state and the client ports must be in Unlocked-enabled service state for complete loopback functionality. A facility 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 would show the AS-MT condition, which indicates that all alarms are suppressed on the port during loopback testing.)

1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks

Facility loopbacks and terminal 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 or TXP loopback tests differ from other testing in that loopback testing does not require circuit creation. MXP or 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.

You can use these procedures on transponder cards (TXP, TXPP) or muxponder cards (MXP, MXPP) cards. The example in this section tests an MXP or TXP circuit on a three-node bidirectional line switched ring (BLSR) or multiswitched path ring (MS-SPRing). Using a series of facility loopbacks and terminal loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains six network test procedures:

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

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

1. A facility loopback on the source-node MXP or TXP port

2. A terminal loopback on the source-node MXP or TXP port

3. A facility loopback on the intermediate-node MXP or TXP port

4. A terminal loopback on the intermediate-node MXP or TXP port

5. A facility loopback on the destination-node MXP or TXP port

6. A terminal 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 Loopback on a Source-Node MXP or TXP Port

This facility loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source muxponder or transponder port under test is located in the source node. Facility loopback can be performed at the trunk port or at a client port. Completing a successful facility loopback on this port isolates the source MXP or TXP port as a possible failure point. Figure 1-3 shows the facility loopback examples on source ONS node TXP ports (client and trunk).

Figure 1-3   Facility Loopback on a Circuit Source MXP or TXP Port
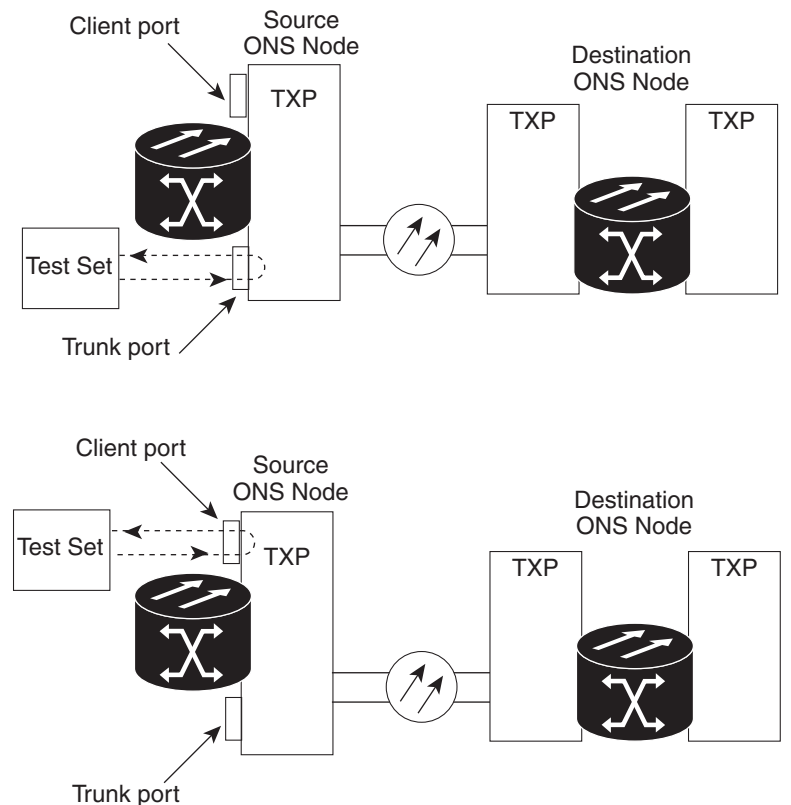
Caution Performing a loopback on an in-service circuit is service-affecting.

> ✎
> **Note**   Facility loopbacks require on-site personnel.

Complete the "Create the Facility Loopback on the Source-Node MXP or TXP Port" procedure on page 1-8.

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

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

> ✎
> **Note**   For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

Use appropriate cabling to attach the transmit (Tx) and receive (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. (Refer to manufacturer instructions for test set use.)

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

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

Step 5   Choose **OOS,MT** (or **locked,maintenance**) 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 the "LPBKFACILITY (ESCON)" condition on page 2-83, "LPBKFACILITY (FC)" condition on page 2-83, "LPBKFACILITY (GE)" condition on page 2-84, "LPBKFACILITY (ISC)" condition on page 2-84 or the "LPBKFACILITY (TRUNK)" condition on page 2-85 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 Loopback Circuit" procedure on page 1-8.

Test and Clear the MXP or TXP Facility 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 no errors, no further testing is necessary with the facility loopback. Clear the facility loopback:

   a.   Click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service 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 "Test the MXP or TXP Card" procedure on page 1-9.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-154 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. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 2 Resend test traffic on the loopback circuit with a known-good card installed.

Step 3 If the test set indicates no errors, the problem was probably the defective card. Return the defective card to Cisco through the Return Materials Authorization (RMA) process. Contact Cisco Technical Support (1 800 553-2447).

**Step 4** Complete the "Physically Replace a Card" procedure on page 2-154 for the faulty card.

Step 5 Clear the facility loopback:

a. Click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service 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 "1.2.2 Perform a Terminal Loopback on a Source-Node MXP or TXP Port" procedure on page 1-9.

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

The terminal loopback test is performed on the node source MXP or TXP muxponder or transponder port. For the circuit in this example, it is the source TXP trunk port or a client port in the source node. Completing a successful terminal loopback to a node source port verifies that the circuit is through the source port. Figure 1-4 shows an example of a terminal loopback on a source TXP port and a client TXP port.

Figure 1-4   *Terminal Loopback on a Source-Node MXP or TXP Port*
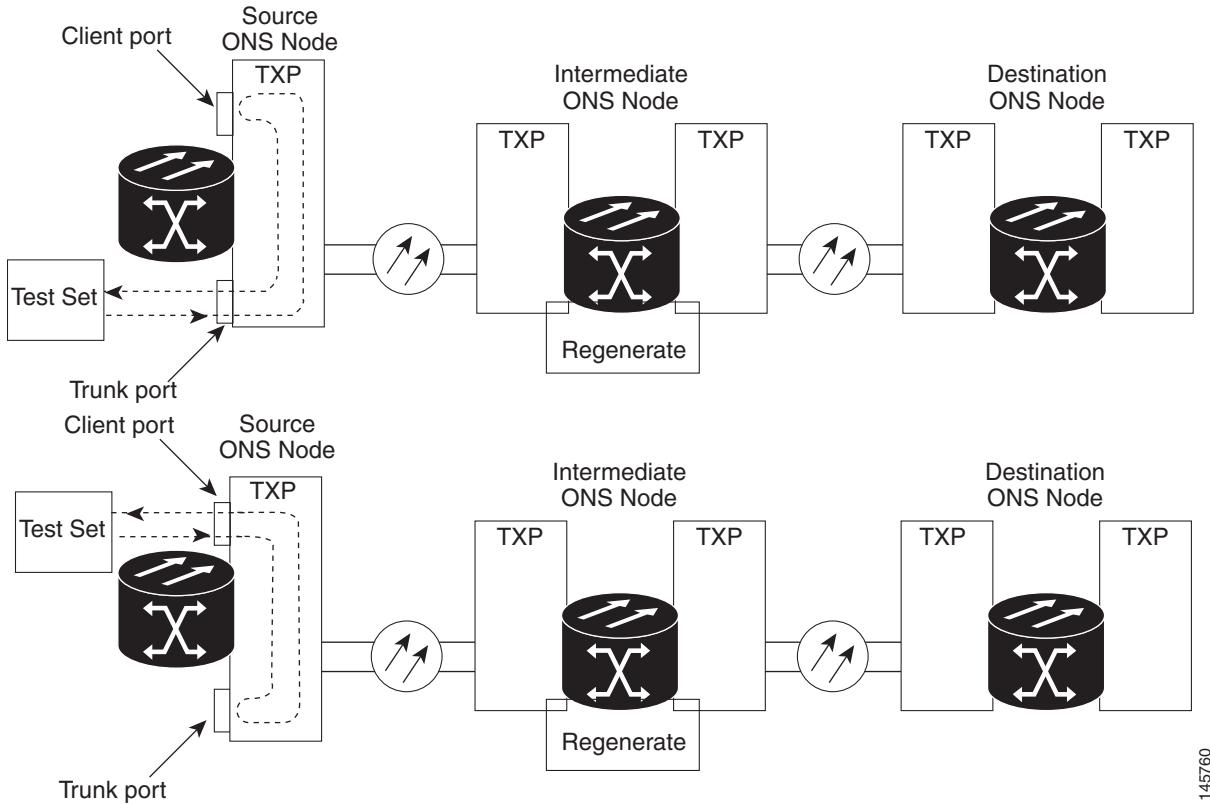
⚠️

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

✎

Note   Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal Loopback on a Source-Node MXP or TXP Port" procedure on page 1-10.

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

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

✎

Note   For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

a.   If you just completed the "1.2.1 Perform a Facility Loopback on a Source-Node MXP or TXP Port" procedure on page 1-7, leave the optical test set hooked up to the MXP or TXP port in the source node.

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. (Refer to manufacturer instructions for test set use.)

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

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

Step 5 Select **OOS,MT** (or **locked,maintenance**) 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 1-11.

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 no errors, no further testing is necessary on the loopback circuit. Clear the terminal loopback state on the port:

a. Double-click the card in the source node with the terminal loopback.

b. Click the **Maintenance > Loopback** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 4 Complete the "Test the MXP or TXP Card" procedure on page 1-11.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-154 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. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

Step 2   Resend test traffic on the loopback circuit with a known-good card.

Step 3   If the test set indicates no errors, 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 Card" procedure on page 2-154 for the defective card.

Step 5   Clear the terminal loopback on the port before testing the next segment of the network circuit path:

    a.   Double-click the card in the source node with the terminal loopback.

    b.   Click the **Maintenance > Loopback** tabs.

    c.   Select **None** from the Loopback Type column for the port being tested.

    d.   Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

    e.   Click **Apply**.

    f.   Click **Yes** in the confirmation dialog box.

Step 6   Complete the "1.2.3 Create a Facility Loopback on an Intermediate-Node MXP or TXP Port" procedure on page 1-12.

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

Performing the facility loopback test on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in Figure 1-5, the test is being performed on an intermediate MXP or TXP port.

Figure 1-5   *Facility Loopback on an Intermediate-Node MXP or TXP Port*
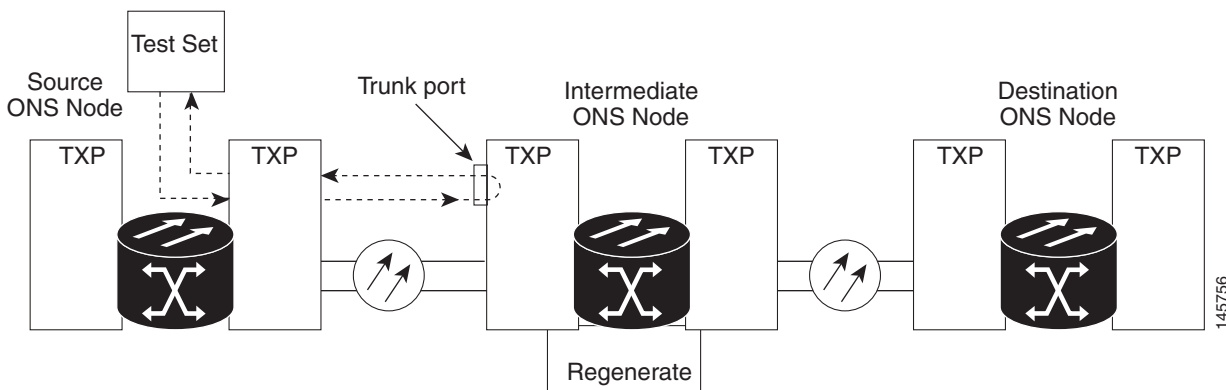
⚠

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

✎

Note   Facility loopbacks require on-site personnel.

Complete the "Create a Facility Loopback on an Intermediate-Node MXP or TXP Port" procedure on page 1-13.

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

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

✎

Note   For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

a.   If you just completed the "1.2.2 Perform a Terminal 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 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. (Refer to manufacturer instructions for test set use.)

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

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

Step 5   Select **OOS,MT** (or **locked,maintenance**) 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 Loopback Circuit" procedure on page 1-13.

Test and Clear the MXP or TXP Port Facility 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 no errors, no further testing is necessary with the facility loopback. Clear the facility loopback from the port:

a.   Click the **Maintenance > Loopback** tabs.

b.   Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service 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 "Test the MXP or TXP Card" procedure on page 1-14.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-154 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. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

Step 2 Resend test traffic on the loopback circuit with a known-good card installed.

Step 3 If the test set indicates no errors, 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 Card" procedure on page 2-154 for the faulty card.

Step 5 Clear the facility loopback from the port:

a. Click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service 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 "1.2.4 Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports" procedure on page 1-14.

1.2.4 Create a Terminal 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 intermediate client or trunk port is causing circuit trouble. In the example situation in Figure 1-6, the terminal loopback is performed on an intermediate MXP or TXP port in the circuit. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

Figure 1-6   Terminal Loopback on an Intermediate-Node MXP or TXP Port
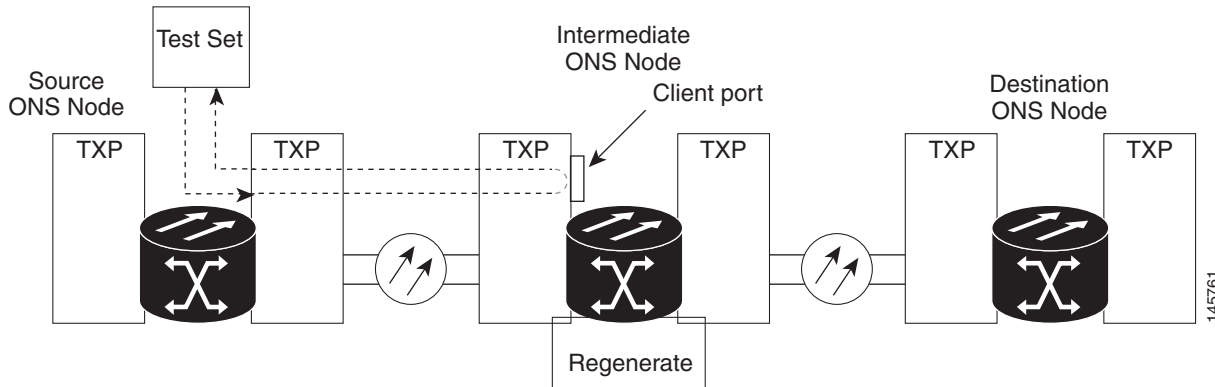
⚠️

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

✏️

Note   Terminal loopbacks require on-site personnel.

Complete the "Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports" procedure on page 1-15.

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   For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

  a. If you just completed the "1.2.3 Create a Facility Loopback on an Intermediate-Node MXP or TXP Port" section on page 1-12, 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. (Refer to manufacturer instructions for test set use.)

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 drop-down list 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** tabs.

  d. Select **OOS,MT** (or **locked,maintenance**) 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 1-16.

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 no errors, 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** tabs.

    c. Select **None** from the Loopback Type column for the port being tested.

    d. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

    e. Click **Apply**.

    f. Click **Yes** in the confirmation dialog box.

Step 4 Complete the "Test the MXP or TXP Card" procedure on page 1-16.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-154 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. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 2 Resend test traffic on the loopback circuit with a known-good card.

Step 3 If the test set indicates no errors, 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 Card" procedure on page 2-154 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** tabs.

   c. Select **None** from the Loopback Type column for the port being tested.

   d. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

   e. Click **Apply**.

   f. Click **Yes** in the confirmation dialog box.

Step 6   Complete the "1.2.5 Perform a Facility Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-17.

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

You perform a facility loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-7 shows a facility loopback being performed on a TXP client or trunk port at a destination node.

Figure 1-7   Facility Loopback on a Destination-Node MXP or TXP Port
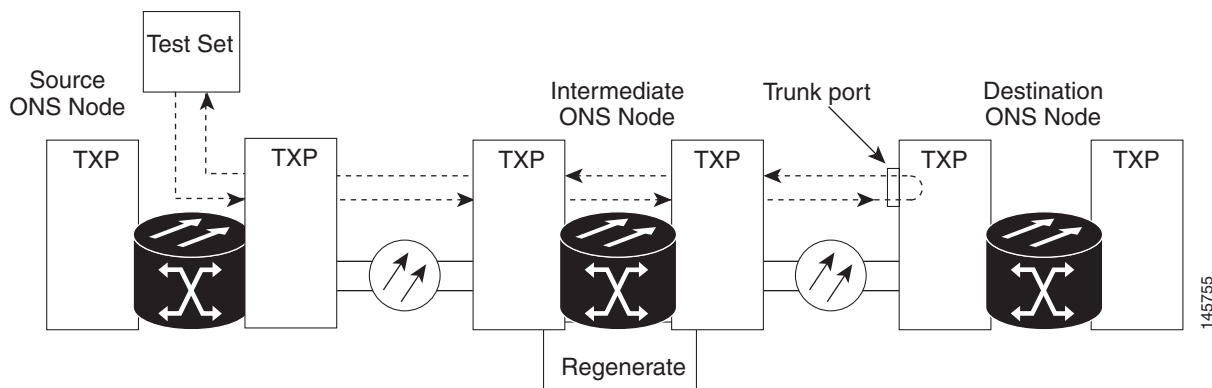
⚠
Caution   Performing a loopback on an in-service circuit is service-affecting.

✎
Note   Facility loopbacks require on-site personnel.

Complete the "Create the Facility Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-18.

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

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

✎

Note   For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

    a.   If you just completed the "1.2.4 Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports" procedure on page 1-14, 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. (Refer to manufacturer instructions for test set use.)

Step 3   Create the facility 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 drop-down list 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** tabs.

    d.   Select **OOS,MT** (or **locked,maintenance**) 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 Loopback Circuit" procedure on page 1-18.

Test and Clear the MXP or TXP Facility 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 no errors, no further testing is necessary with the facility loopback. Clear the facility loopback from the port:

    a.   Click the **Maintenance > Loopback** tabs.

    b.   Choose **None** from the Loopback Type column for the port being tested.

    c.   Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service 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 "Test the MXP or TXP Card" procedure on page 1-19.

Test the MXP or TXP Card

Step 1   Complete the "Physically Replace a Card" procedure on page 2-154 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. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

Step 2   Resend test traffic on the loopback circuit with a known-good card installed.

Step 3   If the test set indicates no errors, 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 Card" procedure on page 2-154 for the faulty card.

Step 5   Clear the facility loopback on the port:

    a.   Click the **Maintenance > Loopback** tabs.

    b.   Choose **None** from the Loopback Type column for the port being tested.

    c.   Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service 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 "1.2.6 Perform a Terminal Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-19.

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 1-8 shows a terminal loopback on an destination node TXP port.

Figure 1-8   *Terminal Loopback on a Destination-Node MXP or TXP Port*
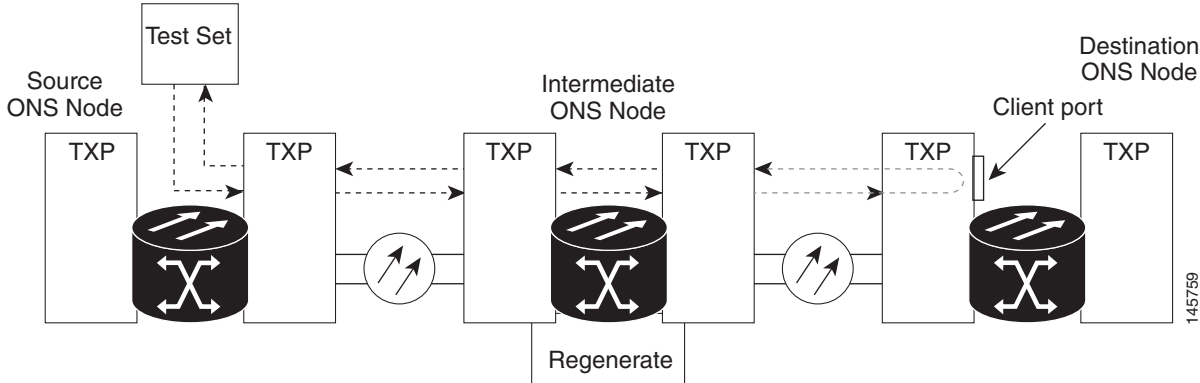
⚠️
Caution   Performing a loopback on an in-service circuit is service-affecting.

✎
Note   Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-20.

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   For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

    a.   If you just completed the "1.2.5 Perform a Facility Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-17, 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. (Refer to manufacturer instructions for test set use.)

✎
Note   It is normal for the "LPBKTERMINAL (ESCON)" condition on page 2-85, "LPBKTERMINAL (FC)" condition on page 2-86, "LPBKTERMINAL (GE)" condition on page 2-86, "LPBKTERMINAL (ISC)" condition on page 2-87 or the "LPBKTERMINAL (TRUNK)" condition on page 2-87 to appear during loopback setup. The condition clears when you remove the loopback.

Step 3   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 drop-down list 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** tabs.

    d. Select **OOS,MT** (or **locked,maintenance**) 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 1-21.

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 no errors, 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** tabs.

    c. Select **None** from the Loopback Type column for the port being tested.

    d. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin 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 errors, the problem might be a faulty card.

Step 5 Complete the "Test the MXP or TXP Card" procedure on page 1-21.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-154 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. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 2 Resend test traffic on the loopback circuit with a known-good card.

Step 3 If the test set indicates no errors 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 Card" procedure on page 2-154 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** tabs.

   c. Select **None** from the Loopback Type column for the port being tested.

   d. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

   e. Click **Apply**.

   f. 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 ITU-T 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 ITU-T G.709 OTN using PM and TCAs.

1.3.1 G.709 Monitoring in Optical Transport Networks

Recommendation ITU-T G.709 is part of a suite of recommendations covering the full functionality of an OTN. ITU-T G.709 enables single-wavelength SONET transparent optical wavelength-based networks. ITU-T G.709 adds the Operation, Administration, Maintenance, and Provisioning (OAM&P) functionality of SONET/SDH to DWDM optical networks. It adds extra overhead to existing SONET, Ethernet, or asynchronous transfer mode (ATM) bit streams for performance management and improvement.

Like traditional SONET networks, ITU-T G.709 optical networks have a layered design (Figure 1-9). This structure enables localized monitoring that helps you isolate and troubleshoot network problems.

Figure 1-9   *Optical Transport Network Layers*
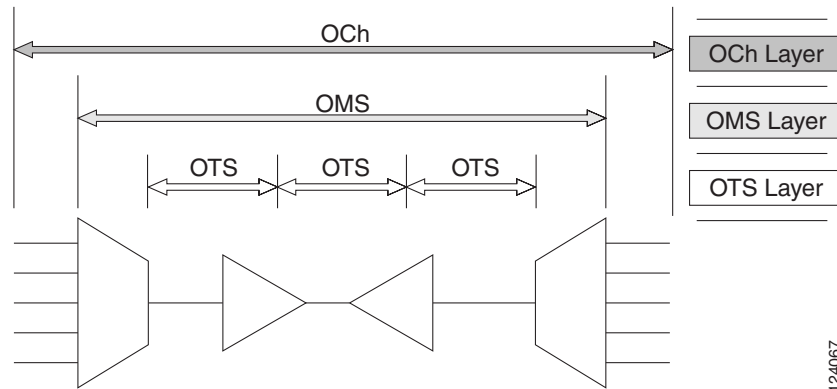
1.3.2 Optical Channel Layer

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, ATM, Fibre 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 32MUX-O card and an optical demultiplexer such as the 32DMX-O card.

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 32MUX-O card and an amplifier such as the OPT-PRE card

- An amplifier and another amplifier, such as the OPT-BST card and the OPT-PRE card

- An amplifier such as the OPT-BST card and a demultiplexer such as the 32DMX card

1.3.5 Performance Monitoring Counters and Threshold Crossing Alerts

PM counters and TCAs can be used for identifying trouble and troubleshooting problems in ITU-T 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 that contains greater than or equal to 30 percent 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 PM count parameters are associated with different read points in a network. Figure 1-10 illustrates the PM read points that are useful in identifying DWDM circuit points of failure. Chapter 5, "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 PM 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 1-10   Performance Monitoring Points on ONS DWDM*
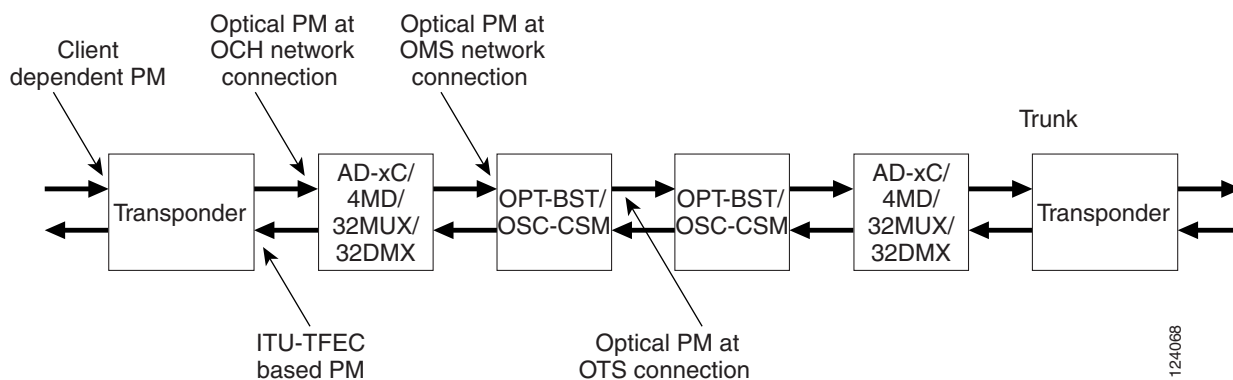
TCAs are used to monitor performance through the management interface by indicating whether preset thresholds have been crossed, or whether a transmission (such as a laser transmission) is degraded. TCAs are not associated with severity levels. They are usually associated with rate, counter, and percentage parameters that are available at transponder monitoring points. Chapter 5, "Performance Monitoring," contains more information about these alerts.

Select and complete the following procedures according to your network parameters.

Set Node Default BBE or SES Card Thresholds

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

Step 1   In node view, click the **Provisioning > Defaults** tabs (Figure 1-11).

Figure 1-11   Set Default BBE/SES Card Thresholds
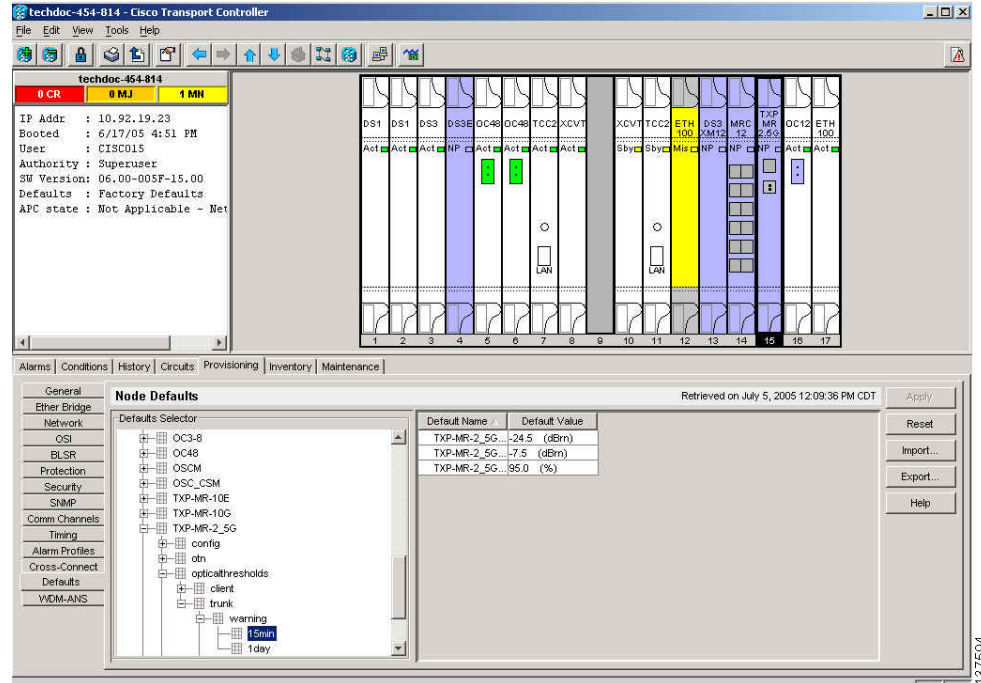
Step 2   In the Defaults Selector field, click the transponder or muxponder card you wish to provision, then click **opticalthresholds > trunk > warning > 15min** in the drop-down list.

Provision Individual Card BBE or SES Thresholds in CTC

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

Step 1   In node view, double-click the applicable transponder or muxponder card (TXP_MR_10G, TXPP_MR_2.5G, or MXP_2.5G_10G.)

Step 2   Click the **Provisionin**g > **OTN** > **G.709 Thresholds** tabs (Figure 1-12).

Figure 1-12   Provision Card BBE/SES Thresholds
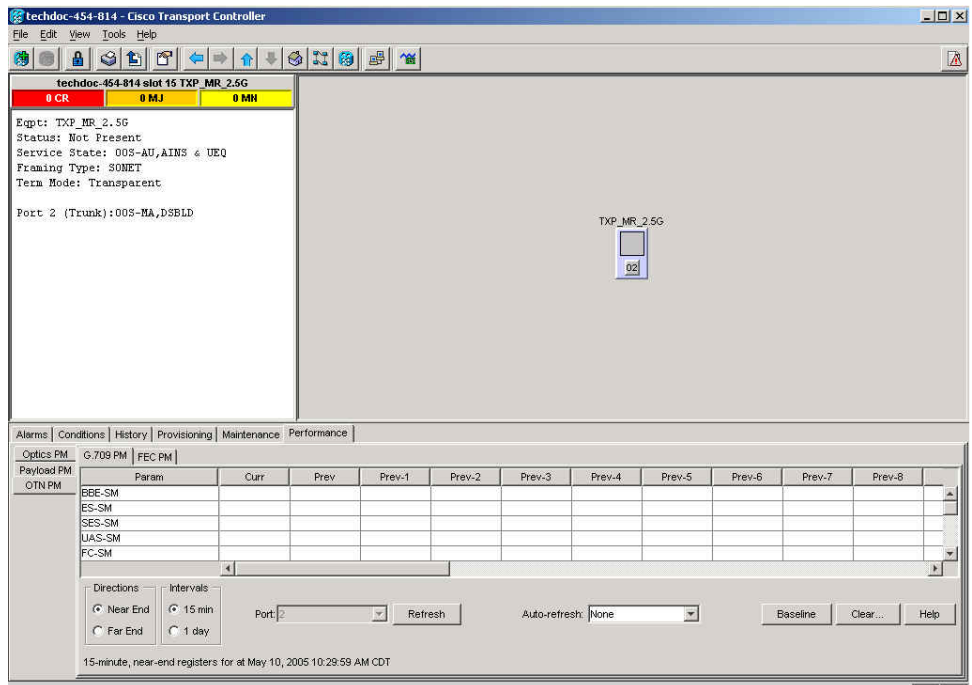
Step 3   In the Directions area, click the **Near End** radio button.

Step 4   In the Intervals area, click the **15 Min** radio button.

Step 5   In the Types area, click the **PM (ODUk)** radio button.

Step 6   In the SES and BBE fields, enter threshold numbers, for example 500 and 10000.

Provision Card PM Thresholds Using TL1

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

Step 1   Open a TL1 command line (click **Tools > Open TL1 Connection**).

Step 2   On the TL1 command line, use the following syntax:

SET-TH-OCH:[<TID>]:<AID>:<CTAG>::<MONTYPE>,<THLEV>,[<LOCN>],,[<TMPER>];

where:

- Access Identifier (AID) identifies the NE to which the command pertains. All the STS, VT1, facility and DS1 AIDs are supported.

- The parameter MONTYPE is the monitored type.

- The parameter THLEV is optional and indicates a threshold count value (the number of errors which must be exceeded before the threshold is crossed).

- The parameter LOCN specifies the location associated with the particular command.

- The parameter TMPER 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 more information about this command and a list of TL1 commands, refer to the
Cisco SONET TL1 Command Guide at the following link:
http://www.cisco.com/en/US/products/hw/optical/ps2006/products_command_reference_book
09186a0080483b9b.html

Provision Optical TCA Thresholds

Complete the following procedure to provision TCA thresholds in CTC.

Step 1   In card view, click the **Provisioning > Optics Thresholds** tabs (Figure 1-13).

Figure 1-13   Provision Optical TCA Thresholds
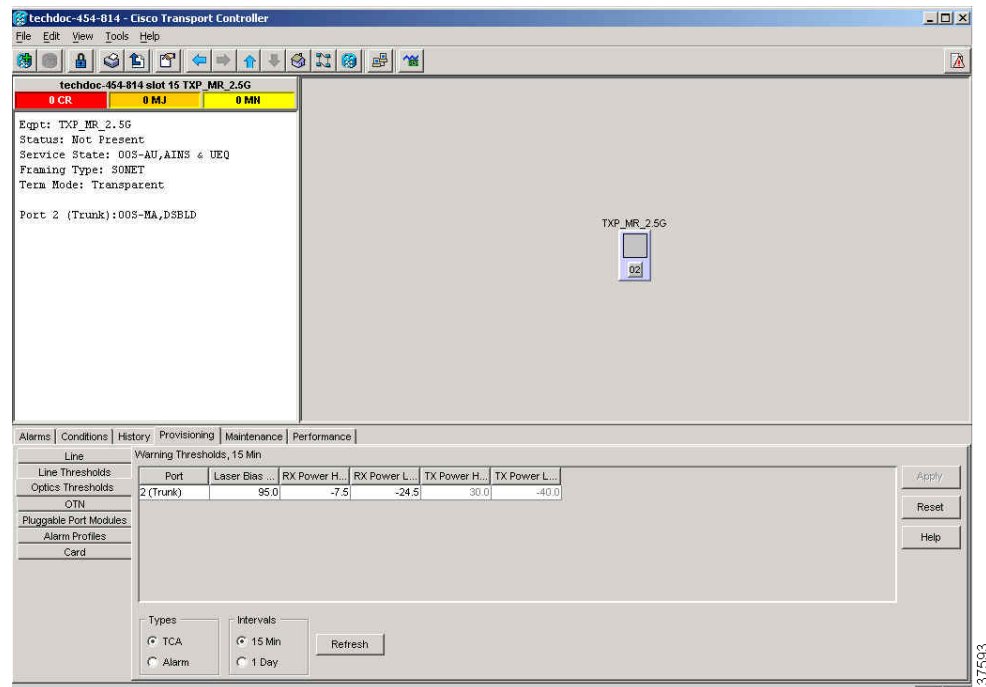
Step 2   In the Types area, click **TCA**.

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.

1.3.6 Forward Error Correction

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

- BIT-EC—Bit errors corrected (BIT-EC) 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 BIT-EC and UNC-WORDS PM parameters for FEC.

Provision Card FEC Thresholds

Step 1 In node view, double-click a transponder or muxponder card to open the card view. (In this example, cards such as the TXP_MR_10G, TXPP_MR_2.5G, and MXP_2.5G_10G are applicable.)

Step 2 Click the **Provisioning** > **OTN** > **FEC Thresholds** tabs (Figure 1-14).

Figure 1-14   Provision Card FEC Thresholds
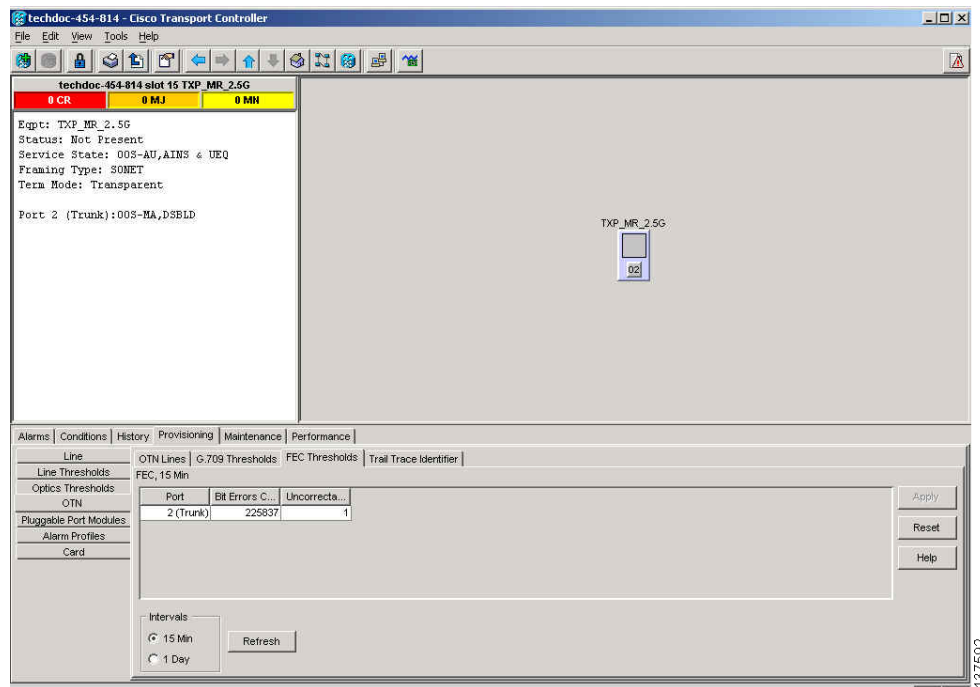
Step 3 In the Bit Errors Corrected field, enter a threshold number, for example 225837.

Step 4 In the Uncorrectable Words field, enter a threshold number, for example, 2.

Step 5 In the Intervals area, click **15 Min**.

1.3.7 Sample Trouble Resolutions

The following sample trouble resolutions use PM and TCAs to isolate degrade points.

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 patchcord between the transponder and the DWDM port.

Recommended Action   Check the patchcord on the transponder DWDM port.

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

Recommended Action   Check the connector on the OCH port of the ADxC-xx.x card.

Possible Cause   There are dirty client connectors on the ADxC-xx.x card 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 an ADxB-xx.x card.

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-xx.x card port.

Recommended Action   Check the connector on the drop port of the 4MD-xx.x card.

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

Recommended Action   Check the connector on the drop port of the ADxB-xx.x card.

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

Recommended Action   Check the patchcord on the 4MD-xx.x or AD1B-xx.x card.

Possible Cause   There is a degraded patchcord between the ADxB-xx.x and 4MD-xx.x cards.

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

Symptom   There is a BBE TCA on all transponders that 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 Procedure Guide* for more information about configurations and acceptance tests for this area.

Symptom   You have a laser bias current (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 Software Release 6.0, CTC provides diagnostics for the following functions:

- Verifying proper card ASIC functionality
- Verifying standby card operation
- Verifying proper card LED operation
- Diagnostic circuit creation
- Customer problem notifications detected by alarms
- Provision of a downloadable, machine-readable diagnostic information file to be used by Cisco Technical Support

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 windows. Other diagnostic functions—verifying card LED function, creating bidirectional 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 turn-up, 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 Card LED Operation

Step 1   In node view, click the **Maintenance > Diagnostic** tabs (Figure 1-15).

Figure 1-15   CTC Node View Diagnostic Window
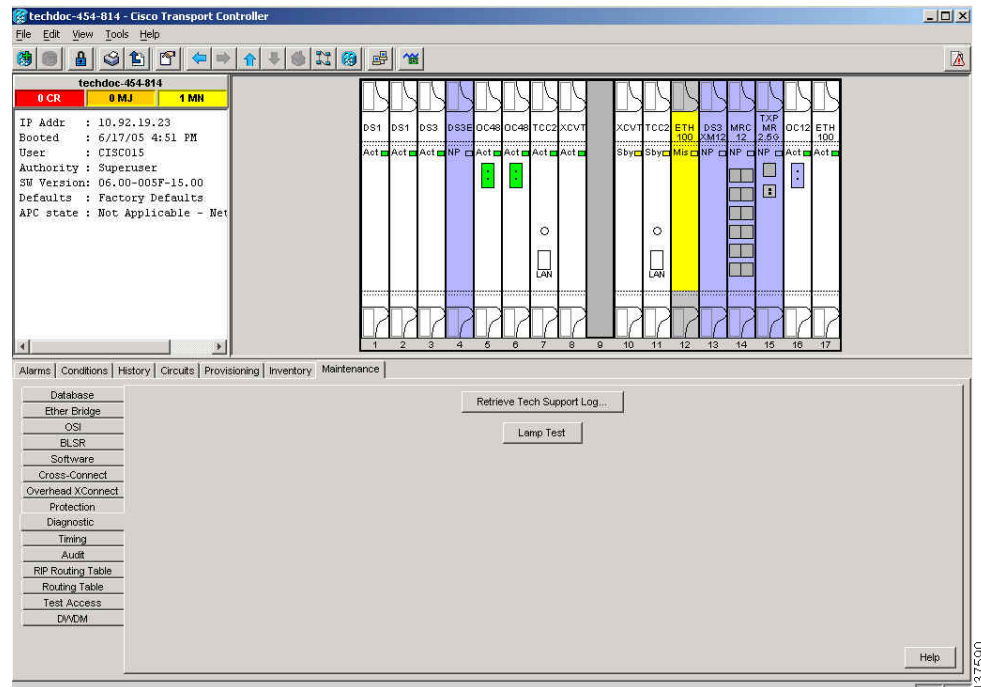
Step 2   Click **Lamp Test**.

Step 3   Watch to make sure all the port LEDs illuminate simultaneously for several seconds, with the following durations:

- For tri-color LEDs: three 5-second cycles
- For dual-color LEDs: one 5-second cycle and one 10-second cycle
- For the AIC or AIC-I: one 15-second cycle

Step 4   Click **OK** in the Lamp Test Run dialog box.

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 icon]

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 "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Off-Load the Diagnostics File

Step 1   In node view, click the **Maintenance > Diagnostic** tabs (Figure 1-15).

Step 2   Click **Retrieve Tech Support Log**.

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 a compressed file (gzip) that can be unzipped and read by Cisco Technical Support.

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**.

1.5 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 do not function properly or have incorrect data.

Possible Cause Incorrect or corrupted node database.

Recommended Action Complete the procedures in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

1.6 PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and Java Runtime Environments (JREs) for Software R6.0, and troubleshooting procedures for PC and network connectivity to the ONS 15454.

1.6.1 PC System Minimum Requirements

Workstations running CTC Software R6.0 for the Optical Networking System (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 Software R6.0 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 R6.0 supports the following platforms:

- Windows NT

- Windows 98

- Windows XP

- Windows 2000

- Solaris 8

- Solaris 9

Software R6.0 supports the following browsers and JREs:

- Netscape 7 browser (PC or Solaris 8 or 9 with Java plug-in 1.4.2)

- PC platforms with Java plug-in 1.4.2

- Internet Explorer 6.0 browser (on PC platforms with Java plug-in 1.4.2)

- Mozilla 1.7 (Solaris only)

Note   You can obtain browsers at the following URLs:

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

- Internet Explorer: http://www.microsoft.com

- Mozilla: http://mozilla.org

Note   The required JRE version is JRE 1.4.2. It is compatible with R4.6 and later.

Note   JRE 1.4.2 for Windows and Solaris is available on Software R6.0 product CDs.

Cisco ONS 15454 DWDM Troubleshooting Guide, R6.0

1.6.4 Unsupported Platforms and Browsers

Software R6.0 does not support the following platforms:

- Windows 95
- Solaris 2.5
- Solaris 2.6

Software R6.0 does not support the following browsers and JREs:

- Netscape 4.73 for Windows.
- Netscape 4.76 on Solaris.
- Netscape 7 on Solaris 8 or 9 is only supported with JRE 1.4.2.

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 entered 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 1-34.

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 1-34. 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 **ipconfig** and press the **Enter** key.

The Windows IP configuration information appears, including the IP address, the 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 1-35 and the "Reconfigure the Browser" procedure on page 1-35.

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:

  a.   Run the Cisco ONS 15454 software CD.

  b.   Open the *CD-drive*:\Windows\JRE folder.

  c.   Double-click the **j2re-1_4_2-win** icon to run the JRE installation wizard.

  d.   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:

  a.   From the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

  b.   In the Preferences window, click the **Advanced > Proxies** categories.

  c.   In the Proxies window, click the **Direct connection to the Internet** check box and click **OK**.

  d.   From the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

    e. In the Preferences window, click the **Advanced > Cache** categories.

    f. 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/XP: **C:\ProgramFiles\Netscape***username***\Communicator\cache**

    g. If the Disk Cache Folder field is not correct, click **Choose Folder**.

    h. Navigate to the file listed in Step f, and click **OK**.

    i. Click **OK** in the Preferences window and exit the browser.

Step 3 If you are using Internet Explorer:

    a. From the Internet Explorer menu bar, click the **Tools > Internet Options** menus.

    b. In the Internet Options window, click the **Advanced** tab.

    c. In the Settings menu, scroll down to Java (Sun) and click the **Use Java 2 v1.4.2 for** *applet* (**requires restart**) check box.

    d. Click **OK** in the Internet Options window and exit the browser.

Step 4 Temporarily disable any virus-scanning software on the computer. See the "1.7.4 Browser Stalls When Downloading CTC JAR Files From TCC2/TCC2P Card" section on page 1-41.

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 onto 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 that 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. (For information about installing cable, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

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 "1.9.2.1 Crimp Replacement LAN Cables" section on page 1-52.

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/TCC2P card. A ping command should work if the PC connects directly to the TCC2/TCC2P card or uses a LAN to access the TCC2/TCC2P card. Complete the "Ping the ONS 15454" procedure on page 1-37.

Ping the ONS 15454

Step 1   Display the command prompt:

   a.   If you are using a Microsoft Windows operating system, from the Start Menu choose **Run**, enter **command** in the Open field of the Run dialog box, and click **OK**.

   b.   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 enter:

   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, it demonstrates that 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 The IP Address of the Node is Unknown

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/TCC2P card in the shelf. Connect a PC directly to the remaining TCC2/TCC2P card and perform a hardware reset of the card. The TCC2/TCC2P 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 1-38.

Retrieve Unknown Node IP Address

Step 1   Connect your PC directly to the active TCC2/TCC2P 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/TCC2P card.

Step 4   After the TCC2/TCC2P 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 1-38. 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 entering one of the following commands:

- **netscape -install** (installs Netscape colors for Netscape use)
- **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 1-39 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 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 Set the system or user CTC_HEAP environment variable to increase the memory limits. Complete the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows" procedure on page 1-40 or the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-41 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.

Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows

✎
Note   Before proceeding with the following steps, ensure that your system has a minimum of 1 GB of RAM. If your system does not have a minimum of 1 GB of RAM, contact the Cisco Technical Assistance Center (TAC).

Step 1   Close all open CTC sessions and browser windows.

Step 2   From the Windows **Start** menu, choose **Control Panel > System**.

Step 3   In the System Properties window, click the **Advanced** tab.

Step 4   Click the **Environment Variables** button to open the Environment Variables window.

Step 5   Click the **New** button under the System variables field.

Step 6   Type `CTC_HEAP` in the Variable Name field.

Step 7   Type `512` in the Variable Value field, and then click the **OK** button to create the variable.

Step 8   Again, click the **New** button under the System variables field.

Step 9   Type `CTC_MAX_PERM_SIZE_HEAP` in the Variable Name field.

Step 10   Type `128` in the Variable Value field, and then click the **OK** button to create the variable.

Step 11   Click the **OK** button in the Environment Variables window to accept the changes.

Step 12   Click the **OK** button in the System Properties window to accept the changes.

Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris

Step 1   From the user shell window, kill any CTC sessions and broswer applications.

Step 2   In the user shell window, set the environment variables to increase the heap size.

Example

The following example shows how to set the environment variables in the C shell:

```
% setenv CTC_HEAP 512
% setenv CTC_MAX_PERM_SIZE_HEAP 128
```

1.7.4 Browser Stalls When Downloading CTC JAR Files From TCC2/TCC2P Card

Symptom The browser stalls or hangs when downloading a CTC Java archive (JAR) file from the TCC2/TCC2P 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 1-41.

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 1-42.

Redirect the Netscape Cache to a Valid Directory

Step 1 Launch Netscape.

Step 2 Open the **Edit** menu.

Step 3 Choose **Preferences**.

Step 4 In 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.

Table 1-3 describes the potential cause of the symptom and the solution.

Table 1-3   *Slow CTC Operation or Login Problems*

Possible Problem	Solution
The CTC cache file might be corrupted or might need to be replaced.	Search for and delete cache files. This operation forces the ONS 15454 to download a new set of Java archive (JAR) files to your computer hard drive. Complete the "Delete the CTC Cache File Automatically" procedure on page 1-43 or the "Delete the CTC Cache File Manually" procedure on page 1-44.
Insufficient heap memory allocation.	Increase the heap size if you are using CTC to manage more than 50 nodes concurrently. See the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows" procedure on page 1-40 or the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-41.
	Note To avoid network performance issues, Cisco recommends managing a maximum of 50 nodes concurrently with CTC. To manage more than 50 nodes, Cisco recommends using Cisco Transport Manager (CTM). Cisco does not recommend running multiple CTC sessions when managing two or more large networks.

Delete the CTC Cache File Automatically

⚠

Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting the TC 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** in the initial browser window to clear the CTC cache. Figure 1-16 shows the Delete CTC Cache window.
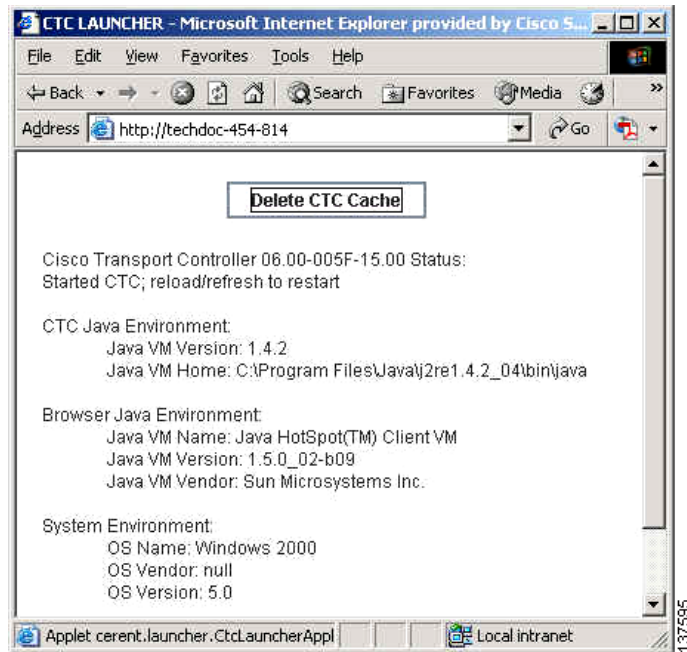
Figure 1-16   Deleting the CTC Cache

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   In the Search Results dialog box, enter **ctc*.jar** or **cms*.jar** in the Search for Files or Folders Named field 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/TCC2P.

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 do not recognize each other.

Recommended Action Correct the core version build as described in the "1.7.9 Different CTC Releases Do Not Recognize Each Other" section on page 1-46.

Possible Cause Username and password do not match.

Recommended Action Correct the username and password as described in the "1.7.10 Username or Password Do Not Match" section on page 1-47.

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 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. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-46. 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 1-4 shows JRE compatibility with ONS 15454 software releases.

Table 1-4   JRE Compatibility

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

Table 1-4   JRE Compatibility (continued)

Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15454 R4.0[1]	No	Yes	No
ONS 15454 R4.1	No	Yes	No
ONS 15454 R4.5	No	Yes	No
ONS 15454 R4.6	No	Yes	Yes
ONS 15454 R4.7	No	Yes	Yes
ONS 15454 R5.0	No	Yes	Yes
ONS 15454 R6.0	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   Enter 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.

1.7.9 Different CTC Releases Do Not Recognize Each Other

Symptom   Different CTC releases do not recognize each other. 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/TCC2P card are incompatible.

Recommended Action   This occurs when the TCC2/TCC2P 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 1-46.

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   Enter 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.

1.7.10 Username or Password Do Not Match

Symptom   A username/password 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/TCC2P card.

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, enter the CISCO15 user name in capital letters, click **Login**, and use the password **otbu+1**, which is case-sensitive.

Complete the "Verify Correct Username and Password" procedure on page 1-47. If the node has been configured for RADIUS authentication, the username and password are verified against the RADIUS server database rather than the security information in the local node database. For more information about RADIUS security, refer to the "Security Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

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.

1.7.11 DCC Connection Lost

Symptom   DCC connection is lost. The node usually has 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.

1.7.12 "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.

1.7.13 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 "Management Network Connectivity" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

1.8 Timing

This section provides solutions to common timing reference errors and alarms.

1.8.1 ONS 15454 Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

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

Possible Cause The optical or 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.

1.8.2 Holdover Synchronization Alarm

Symptom The clock is running at a different frequency than normal and the "HLDOVRSYNC" 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 "HLDOVRSYNC" alarm on page 2-54 for a detailed description.

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

1.8.3 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" alarm on page 2-44 for a detailed description.

1.8.4 Daisy-Chained 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.

1.8.5 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 for 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 "Physically Replace a Card" procedure on page 2-154.

⚠ **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. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations 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 pointer justification (PJ) 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 low optical levels using the "1.9.2 Faulty Fiber-Optic Connections" section on page 1-51.

1.9.2 Faulty Fiber-Optic Connections

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

Possible Cause   Faulty fiber-optic connections. Fiber connection problems usually occur in conjunction with alarms. Refer to the appropriate trouble-clearing procedure in Chapter 2, "Alarm Troubleshooting," to address them.

Recommended Action   Refer to the appropriate trouble-clearing procedure in Chapter 2, "Alarm Troubleshooting," to address them.

Possible Cause   Faulty CAT-5 cables.

Recommended Action   Faulty CAT-5 cables can be the source of alarms and signal errors. Complete the "1.9.2.1 Crimp Replacement LAN Cables" section on page 1-52.

Possible Cause   Faulty Gigabit Interface Converters (GBICs).

Recommended Action   Faulty GBICs can be the source of alarms and signal errors. See the "1.9.2.2 Replace Faulty SFP or XFP Connectors" section on page 1-53.

⚠ **Warning**   **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 272

⚠ **Warning**   **Laser radiation presents an invisible hazard, so personnel should avoid exposure to the laser beam. Personnel must be qualified in laser safety procedures and must use proper eye protection before working on this equipment.** Statement 300

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 1-17 shows the wiring of an RJ-45 connector. Figure 1-18 shows a LAN cable layout, and Table 1-5 shows the cable pinouts. Figure 1-19 shows a cross-over cable layout, and Table 1-6 shows the cross-over pinouts.

Figure 1-17   RJ-45 Pin Numbers

End view of RJ-45 plug   Looking into an RJ-45 jack
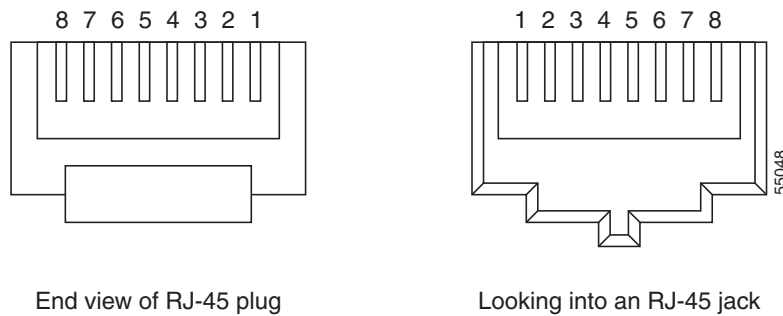
Figure 1-18   LAN Cable Layout
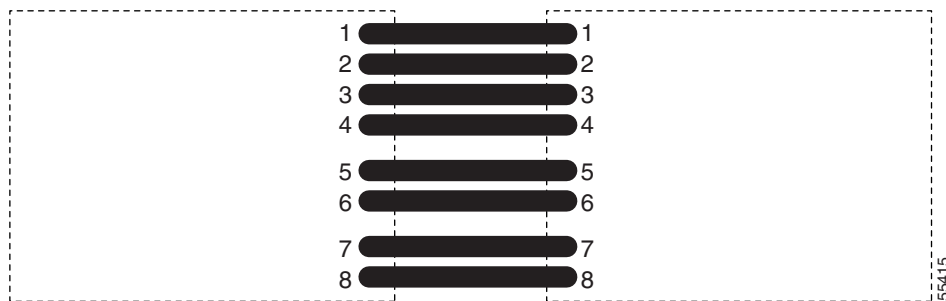
Table 1-5   LAN Cable Pinout

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 1-19   Cross-Over Cable Layout
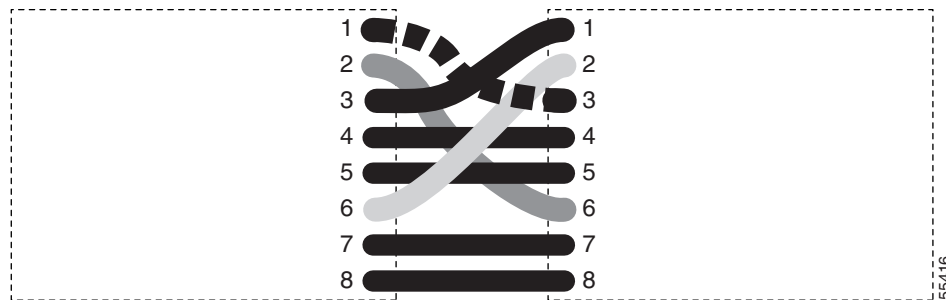
Table 1-6   Cross-Over Cable Pinout

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 SFP or XFP Connectors

Small Form-factor Pluggables (SFPs) and 10-Gbps SFPs (called XFPs) are input/output devices that plug into some transponder and muxponder cards to link the port with the fiber-optic network. The type of SFP or XFP determines the maximum distance that traffic can travel from the card to the next network device. For a description of SFPs and XFPs and their capabilities, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. SFPs and XFPs are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

Warning   **Class 1 laser product.** Statement 1008

Warning   **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 272

Note   SFPs and XFPs must be matched on both ends by type: SX to SX, LX to LX, or ZX to ZX.

Remove SFP or XFP Connectors

Warning   **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 272

Step 1   Disconnect the network fiber cable from the SFP or XFP LC duplex connector.

Step 2   Release the SFP or XFP from the slot by simultaneously squeezing the two plastic tabs on each side.

Step 3   Slide the SFP out of the card slot. A flap closes over the SFP slot to protect the connector on the card.

Install an SFP or XFP Connector

Warning   **Class 1 laser product.** Statement 1008

Warning   **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Step 1   Remove the SFP or XFP from its protective packaging.

Step 2   Check the label to verify that you are using a compatible SFP or XFP for the card where you want to install the connector. Table 1-7 shows the compatible SFPs and XFPs.

Caution   Only use SFPs/XFPs certified for use in Cisco ONSs. The qualified Cisco SFP/XFP pluggable module top assembly numbers (TANs) are provided in Table 1-7.

Table 1-7   *SFP/XFP Card Compatibility*

Card	Compatible SFP/XFP (Cisco Product ID)	Cisco Top Assembly Number (TAN)
MXP_2.5G_10G (ONS 15454 SONET/SDH)	15454-SFP-OC48-IR= ONS-SE-2G-S1=	10-1975-01 10-2017-01
MXP_2.5G_10E (ONS 15454 SONET/SDH)	15454-SFP-OC48-IR= ONS-SE-2G-S1= ONS-SE-2G-L2=	10-1975-01 10-2017-01 10-2013-01
MXP_MR_2.5G MXPP_MR_2.5G	15454-SFP-GE+-LX= 15454E-SFP-GE+-LX= 15454-SFP-GEFC-SX= 15454E-SFP-GEFC-S= ONS-SE-GE-ZX=	10-1832-03 10-1832-03 10-1833-01 10-1833-02

Table 1-7   SFP/XFP Card Compatibility (continued)

Card	Compatible SFP/XFP (Cisco Product ID)	Cisco Top Assembly Number (TAN)
TXP_MR_2.5G (ONS 15454 SONET/SDH) TXPP_MR_2.5G (ONS 15454 SONET/SDH)	15454-SFP3-1-IR= 15454E-SFP-L.1.1= 15454-SFP12-4-IR= 15454E-SFP-L.4.1= 15454-SFP-OC48-IR= 15454E-SFP-L.16.1= ONS-SE-2G-S1= 15454-SFP-200= 15454E-SFP-200= 15454-SFP-GEFC-SX= 15454E-SFP-GEFC-S= 15454-SFP-GE+-LX= 15454E-SFP-GE+-LX= ONS-SE-2G-L2= ONS-SE-GE-ZX=	10-1828-01 10-1828-01 10-1976-01 10-1976-01 10-1975-01 10-1975-01 10-2017-01 10-1750-01 10-1750-01 10-1833-01 10-1833-02 10-1832-01 10-1832-02 10-2013-01
TXP_MR_10E (ONS 15454 SONET/SDH)	ONS-XC-10G-S1	10-2012-01

Step 3   Plug the LC duplex connector of the fiber into a Cisco-supported SFP or XFP.

Step 4   If the new SFP or XFP has a latch, close the latch over the cable to secure it.

Step 5   Plug the cabled SFP or XFP into the card port until it clicks.

To change the payload type of an SFP or XFP (called pluggable port modules [PPMs] in CTC), refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

1.10 Power Supply Problems

This section explains problems related to loss of power or power supply low voltage.

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 1-56.

⚠ **Warning**   **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

⚠ **Warning**   **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

⚠ **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 Electrical Interface Assembly (EIA) under the clear plastic cover.

b.   Verify that the power cable is #10 AWG and in good condition.

c.   Verify that the power cable connections are properly crimped. Stranded #10 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 –40.5 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.

1.11 Power Up Problems for Node and Cards

This section explains power up problems in a node or cards typically caused an improper power supply.

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 "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Reference Manual*.

1.12 Network Level (Internode) Problems

The following network-level troubleshooting is discussed in this section:

- Fiber cut detection
- System restart after a fiber cut
- OCHNC circuit creation failure

Note In the following paragraphs, any reference to the OPT-BST card also includes the OPT-BST-L card.

Prior to following the procedures in this section, pay attention to the following information.

Note The automatic laser shutdown (ALS) function should only be disabled temporarily for installation or maintenance reasons. Activate ALS immediately after maintenance or installation.

The following warning applies to handling unterminated fibers when ALS is disabled:

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

1.12.1 Fiber Cut Detection

A fiber cut is one of the most disruptive faults for a DWDM system because more than one channel is potentially affected. Fault isolation must, therefore, be quick and effective.

In the Multi-Service Transport Platform (MSTP), a dedicated alarm is unambiguously associated with the detection of a fiber cut. The alarm is LOS (OTS or AOTS) and can be raised only by the two cards (OPT-BST and OSC-CSM) that directly interface to the span fiber.

Note Any reference to OPT-BST also refers to OPT-BST-L.

The LOS (OTS or AOTS) alarm is associated with the physical LINE-RX port of the OPT-BST and OSC-CSM cards (in CTC, identified by Port 5 on the OPT-BST and Port 4 on the OSC-CSM). LOS (OTS or AOTS) is the combination of the two alarms LOS-P (OTS or AOTS) (applies to channel payload) and LOS-O (applies to the OC-3 overhead OSC signal).

The simultaneous failure of both the active channel (C- or L-band) and the service channel (1510 nm) coming into the node is evidence of a fiber span issue, whereas either the LOS-P (OTS or AOTS) alarm alone or the LOS-O alarm alone can only be derived from different root causes.

Note   When a fiber cut occurs, the actual conditions on the affected span (for example, alarms raised on both line directions) are strictly dependent on the network ALS setting. The network automatic laser shutdown (ALS) setting is a function of the ALS mode configured on the appropriate cards in the system (OPT-BST, OSC-CSM, and OSCM).

Different symptoms and scenarios can occur, according to the network ALS settings. Consider the linear network (four nodes) in as a reference. The scenarios are presented after the figure.

Figure 1-20   Linear Network, With No Fiber Cut
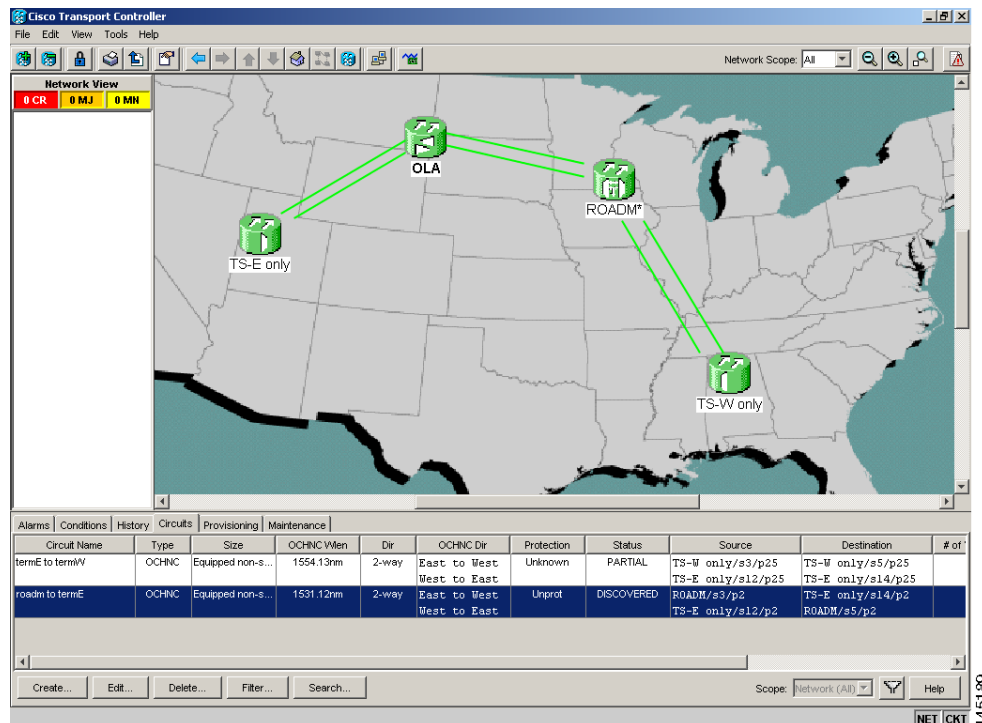
1.12.1.1 Scenario A

Scenario A has the following conditions:

*   ALS Mode = Auto Restart on OPT-BST (+ OSCM) and OSC-CSM
*   Fiber cut on the fiber between the OLA-TX node and the ROADM-RX node

The ALS protocol (refer to the "Network Optical Safety—Automatic Laser Shutdown" section in the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operation Guide*) is activated in the event of a fiber cut, resulting in the shutdown of optical power on both of the fibers belonging to the affected span, even if only one of the two fibers is cut.

The final fault condition of the network is shown in Figure 1-21.

Figure 1-21   Fiber Cut with ALS MODE = Auto Restart
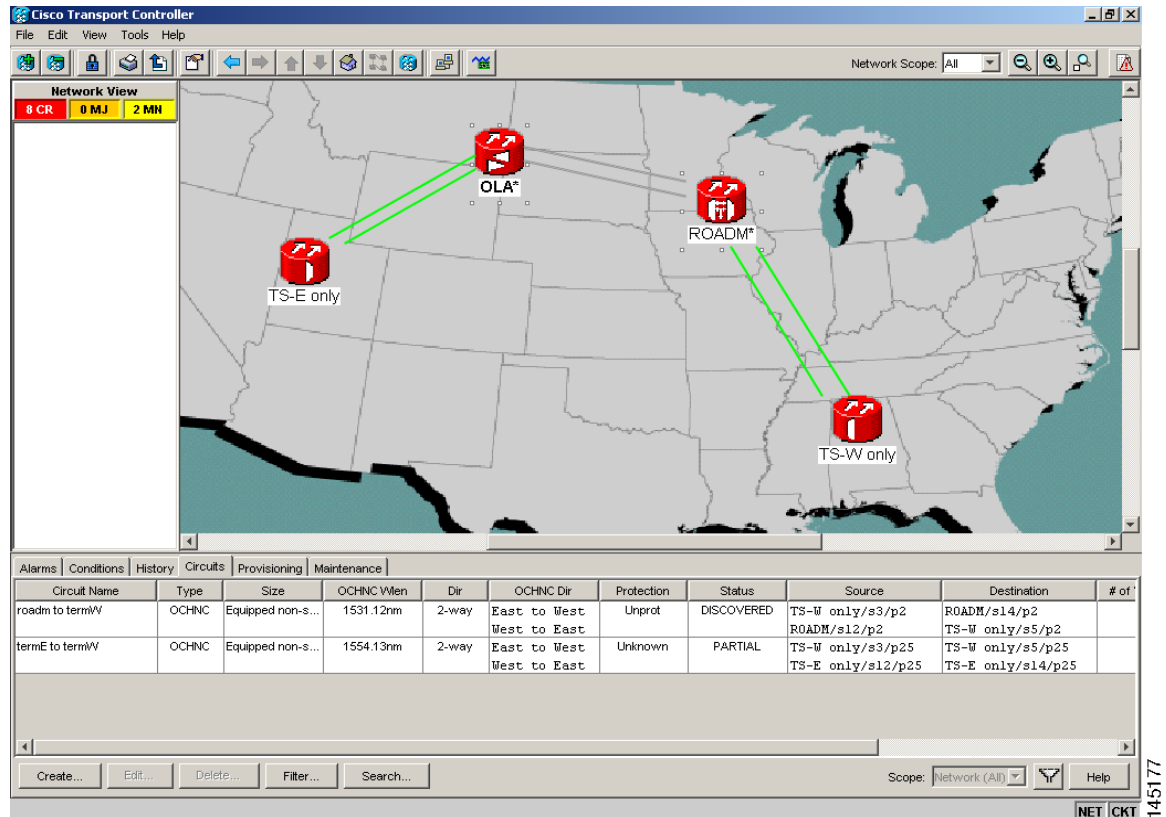
In network view, both of the lines representing the span were formerly green and have now changed to gray. Notice also that the status of all the OCHNC circuits on the broken span have changed from Discovered to Partial.

In node view, the alarm panel of the two nodes (reconfigurable optical add/drop multiplexing [ROADM] and optical line amplification [OLA] in the example) show the LOS (AOTS) alarm on Port 4 of the OSC-CSM (see Figure 1-22) and the LOS (OTS) on Port 5 of the OPT-BST (see Figure 1-23).

Figure 1-22   *LOS Indication on the ROADM Node OSC-CSM*

Figure 1-23   LOS Indication on the OLA Node OPT-BST
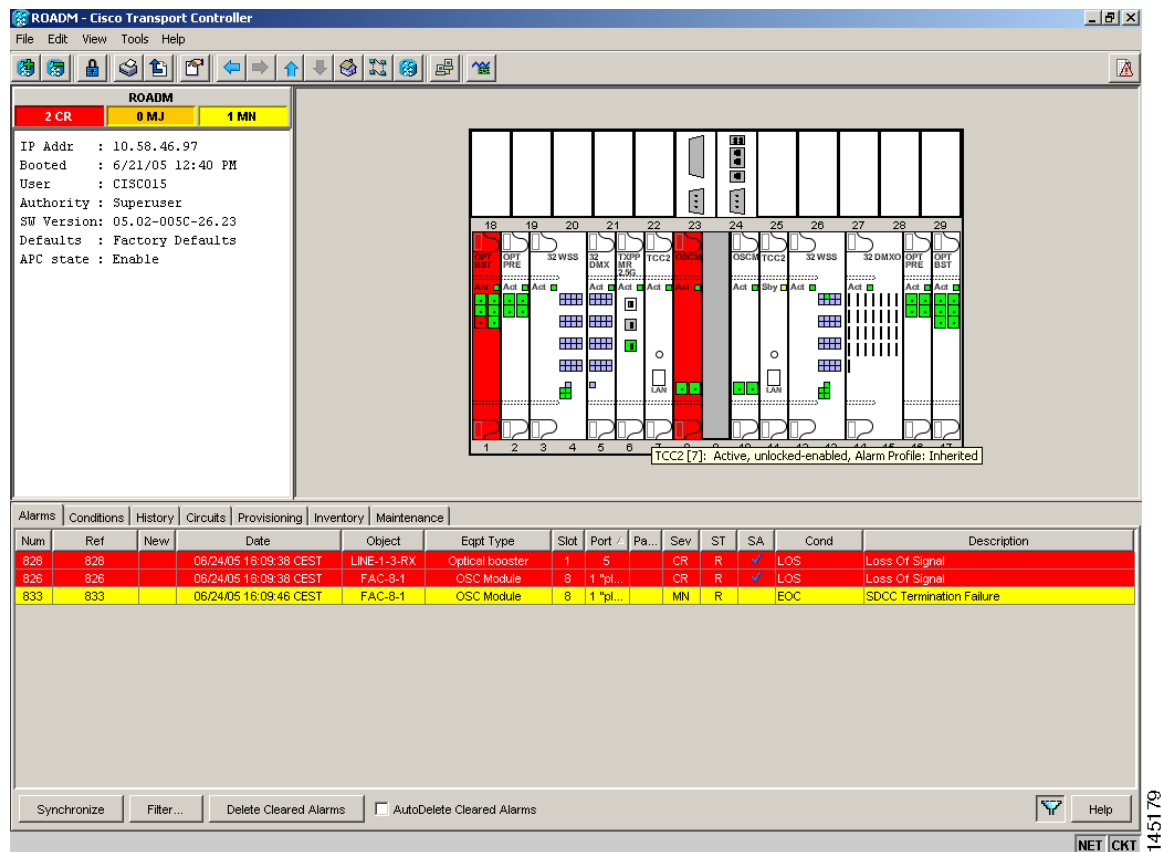
Note An EOC condition is always present on both nodes, because the optical service channel (OSC) link (to which the communication channel applies) is down.

Note For the OSCM card, only an LOS (OC-3) alarm is present at the SONET layer (Port 1).

1.12.1.2 Scenario B

Scenario B has the following conditions:

- ALS Mode = DISABLE on OPT-BST (+ OSCM) and OSC-CSM
- Fiber cut on the fiber between the OLA-TX node and the ROADM-RX node

Because the ALS protocol is disabled, the signal is lost on only the affected fiber (power is not shut down on both fibers).

The LOS (OTS or AOTS) alarm is raised by the ROADM-RX node that was receiving the signal coming from the broken fiber. The final fault condition of the network is shown in Figure 1-24.

Figure 1-24   Network View Fault Condition for Fiber Cut with ALS Mode Disabled
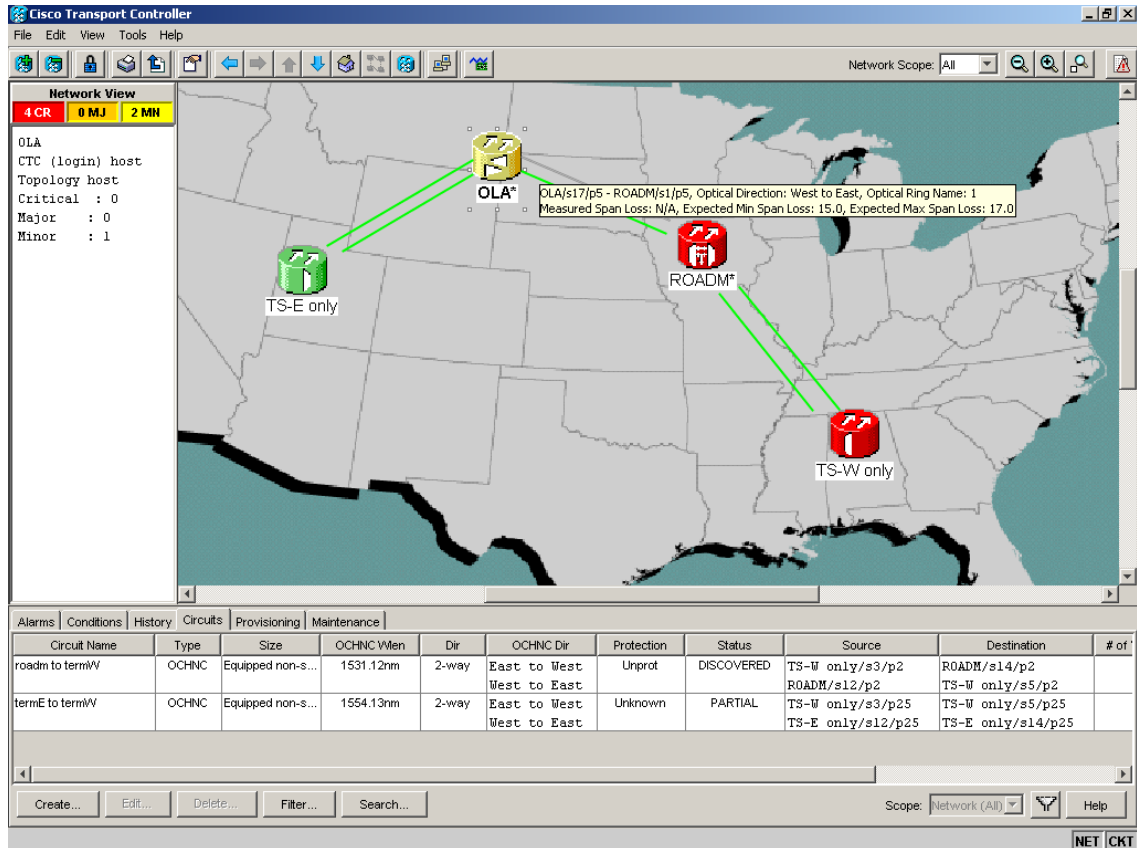
In network view (Figure 1-24), only the actual affected fiber becomes gray, whereas the traffic (and OSC signal as well) on the good fiber is active and fault identification is immediate.

In node views (Figure 1-25 and Figure 1-26), the alarm panel of the receiving node (ROADM in this example) reports the LOS (OTS), while the transmitting node (OLA) reports only an EOC alarm.

Figure 1-25   *ROADM Node View with Fault Condition for ALS MODE Disabled*

Figure 1-26   OLA Node View with Fault Condition for ALS MODE Disabled
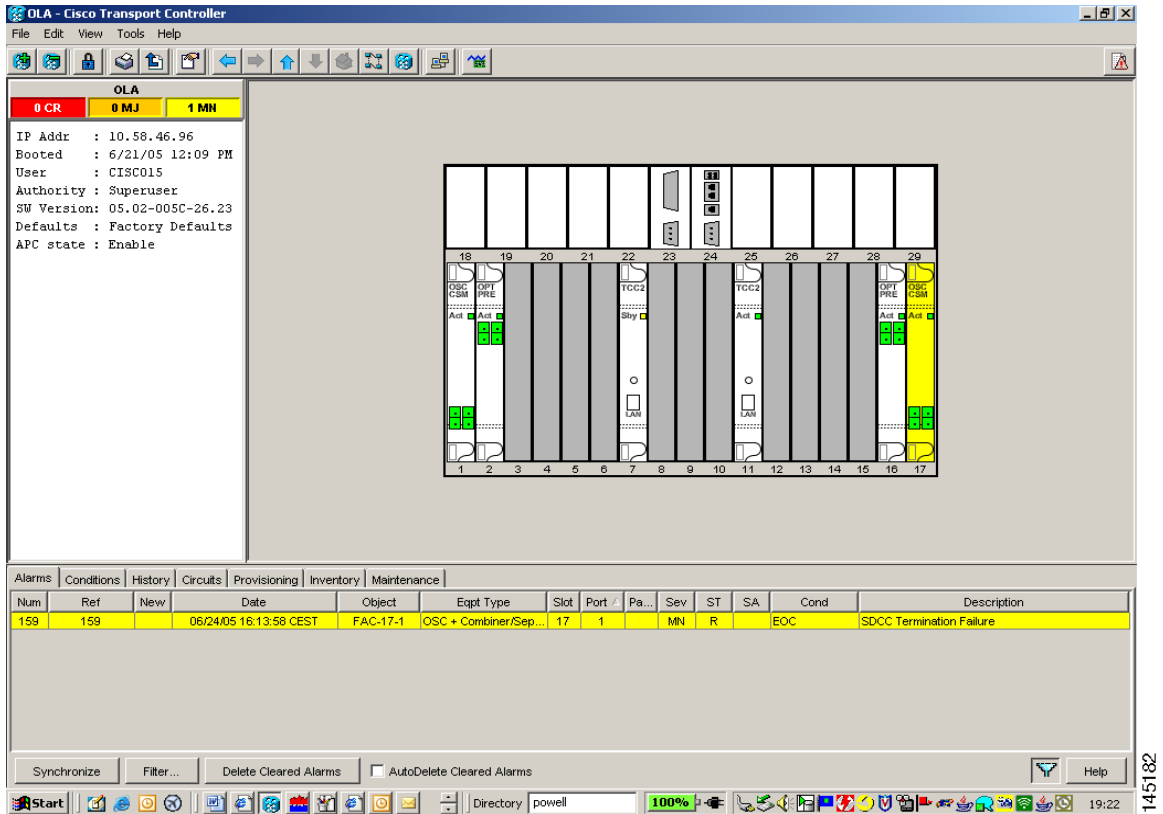
In order to troubleshoot and eventually fix a fiber cut, follow the . The basic assumption is that the MSTP system was already installed and working correctly before the alarm condition occurred. For first installation or restart from a fiber cut, refer to .

Fix a Fiber Cut

⚠

Warning   **When the network ALS setting is DISABLE, optical power is still present at the damaged fiber. Before fixing the span, it is highly recommended that you shut down the amplifier and the OSC laser upstream of the fiber cut.**

Step 1   Isolate the span affected by the fiber cut.

a.   Go to CTC network view.

b.   Identify the span connection that is gray.

Step 2   Verify the alarm is valid, then perform the following steps for both DWDM nodes connected to the span identified in Step 1.

a.   Double-click the card directly connected to the span (either the OPT-BST or the OSC-CSM).

b.   Click the Alarms tab and verify that a LOS condition is present on the LINE-RX port. If the alarm is correctly reported, move to Step 3. If not, close the CTC application, delete the CTC cache and reopen the CTC connection.

c. Click the **Synchronize** button on the bottom left of the window.

> ✎
>
> **Note** If the "gray" condition of the span persists, log into the Technical Support website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a service-affecting problem.

Step 3 If the network ALS setting on the DWDM nodes that you are troubleshooting is Auto Restart, continue with Step 4; if the network ALS setting is DISABLE, go to Step 5.

> ✎
>
> **Note** The network ALS setting is a function of the ALS mode configured on the appropriate cards in the system (OPT-BST, OSC-CSM, and OSCM).

Step 4 Isolate the fiber affected by the fiber cut. For the two fibers belonging to the span, identify the fiber belonging to the west-to-east (W–E) line direction:

a. Go into the upstream node and identify the OSCM or OSC-CSM card managing the OSC termination referring to the faulty span.

b. Double-click the card, then click the **Maintenance Panel** tab.

c. Force the OSC-TX laser to be active by setting the ALS Mode to **DISABLE**.

d. Go into the downstream node and verify if OSC power is being received.

 - If a pair of OPT-BST + OSCM cards terminate the OSC connection, click the **Provisioning > Optical Line > Parameters** tabs, then verify that there is power for OSC-TX (port 4).

 - If an OSC-CSM terminates the OSC connection, click the **Provisioning > Optical Line > Parameters** tabs, then verify that there is power for OSC-RX (port 6).

e. If no power is detected and the LOS (OC-3) alarm persists, go to Step 5; otherwise, the fiber under test is good. In this case, go to Step f to check the other fiber.

f. Repeat Steps a to d for the other fiber to verify that it is at fault.

Step 5 Repair the identified broken fiber to restore the internode link.

1.12.2 System Restart after a Fiber Cut

When the network ALS setting is Auto Restart, the system automatically restarts after a fiber cut occurs. The MSTP system restart after a fiber cut is a fully automatic process regulated by a chronological sequence of steps including the OSC link built-in amplifiers restart and amplifier power control (APC) regulation.

The successful completion of system restart is strictly related to possible changes of the insertion loss value of the repaired span. A change in insertion loss is dependent on many factors, including the process of physically repairing the fiber, a change in fiber length after repair, and so on.

Four different scenarios related to span loss are presented in this section:

1. Span loss increased:

 - Span loss change > 5 dBm

 - OSC power value on the receiver < –42 dBm

2. Span loss increased:

- Span loss change > 5 dBm

- OSC power value on the receiver > –42 dBm

3. Span loss increased: 3 dBm < span loss change < 5 dBm

4. Span loss increased: span loss change < 3 dBm

Note   It is also possible that span loss decreased, but this is unlikely. This condition does not prevent the MSTP system automatic restart process, but can lead (potentially) to issues downstream of the repaired span, for example, a Power Overload condition on the OSC receiver or on the Trunk-RX port of a TXP or MXP card.

These conditions are identified by specific alarms (see the "HI-RX-POWER" section of Chapter 2, "Alarm Troubleshooting" of the *DWDM Alarm and Troubleshooting Guide*).

The symptoms of the possible span loss scenarios (except for span loss decrease) are described in the following paragraphs. Refer to the linear network in Figure 1-20 during the discussion of the scenarios.

The basic assumption is that the network ALS feature (for feature details, refer to the "Network Optical Safety––Automatic Laser Shutdown" section in the *Cisco ONS 15454 DWDM Installation and Operation Guide*) is active (ALS Mode = Auto Restart on the OPT-BST [+ OSCM] and OSC-CSM). Given this assumption, the starting condition is as shown in Figure 1-21.

The system behavior when the network ALS Mode is DISABLE is a subcase that requires a manual restart after repairing a single fiber in only one line direction.

Note   The network ALS feature is a function of the ALS Mode settings of the OPT-BST, OSCM, and OSC-CSM cards. For the network ALS Mode to be disabled, each of these cards must have its ALS Mode set to DISABLE.

1.12.2.1 Scenario 1: Span Loss Change > 5 dBm and OSC Power Value on the Receiver < –42 dBm

The following conditions are present in Scenario 1:

- In network view, both of the lines representing the span remain gray as long as the status of the OCHNC circuits relating to the repaired span remain Partial.

- In node view, the alarm panels of the two nodes (ROADM and OLA in this example) show the LOS (OTS or AOTS) condition on the LINE-RX port of the OPT-BST or OSC-CSM.

- An EOC condition is always present on both nodes because the OSC optical link is down due to an incoming power level lower than the optical sensitivity limit (–42 dBm). The system condition remains unchanged as illustrated in Figure 1-21.

- Every 100 seconds, the ALS protocol turns up the OSC TX laser in a pulse mode (pulse duration = 2 seconds), but the excessive loss on the span prevents the OSC link from synchronizing, and the MSTP system remains unoperational.

Note   During the attempt to restart, a valid power value is reported by the OSC transmit card (in the example, the OSC-CSM in the OLA node), but on the OSC receive card (the OSCM in the ROADM node), the alarm condition persists.

Corrective Action for Scenario 1

Step 1   Follow these steps to verify the alarms for both DWDM nodes connected to the repaired span:

    a.   Double-click the card directly connected to the span (either the OPT-BST or the OSC-CSM).

    b.   Click the **Alarms** tab.

    c.   Verify that a LOS condition is present on the LINE-RX port.

    d.   Click the **Synchronize** button on the bottom left of the window.

    e.   If the alarm is correctly reported, move to Step 2. If not, close the CTC application and delete the CTC cache. Then reopen the CTC connection, and repeat Step 1.

    Note   If the gray color persists on the span, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a service-affecting problem.

Step 2   Isolate the fiber affected by the excessive insertion loss. For the two fibers belonging to the span, identify the one for the W–E line direction.

    a.   Go into the upstream node and identify the OSCM or OSC-CSM card that manages the OSC termination for the faulty span.

    b.   Double-click the card, then click the **Maintenance** tab.

    c.   Force the OSC-TX laser active by setting ALS Mode to **DISABLE**.

    d.   Go into the downstream node and verify the OSC Power level received.

        •   If a pair of OPT-BST + OSCM cards terminate the OSC connection, click the **Provisioning > Optical Line > Parameters** tabs, then verify that there is power for OSC-TX (Port 4).

        •   If an OSC-CSM terminates the OSC connection, click the **Provisioning > Optical Line > Parameters** tabs, then verify that there is power for OSC-RX (Port 6).

        •   If no power is detected and the LOS (OC-3) alarm persists, the faulty fiber has been identified, so go to Step 3.

    e.   If a power value greater than –42 dBm is detected, the fiber under test has been properly repaired. However, it is recommended that you check the new fiber Insertion Loss value.

        •   In node view, click the **Maintenance > DWDM > WDM Span Check** tabs.

        •   Retrieve the new value of fiber Insertion Loss of the repaired span.

    Note   The new value of the fiber Insertion Loss of this fiber after restoration must be less than 5 dB higher than the previous Insertion Loss value. If possible, try to recover the original value by making a better fiber splice. If this is not possible, use the new value (must be less than 5 dB higher than the previous value) and rerun Cisco MetroPlanner to revalidate the new condition.

Step 3   For the two fibers belonging to the repaired span, identify one for the east to west (E–W) line direction.

Step 4   Repeat the procedure starting at Step 2 for the E–W direction.

Step 5   Clean the LINE-RX and LINE-TX connectors for the failing fiber identified in the previous steps.

Step 6   If the problem persists, continue with Step 7. Otherwise, the corrective action is finished.

Step 7   Repair the failing fiber again until the expected OSC link is reestablished.

Note   If the OSC link cannot be reestablished (either by splicing or replacing the fiber), and the new value of Span Loss cannot be modified, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

1.12.2.2 Scenario 2: Span Loss Change > 5 dBm and OSC Power Value on the Receiver > –42 dBm

In network view, both of the lines representing the span change to green; however, the status of the OCHNC circuits relating to the repaired span remains Partial, instead of Complete (due to the fiber cut).

This change is due to the fact the physical optical power value received by the OSC transceiver is above the sensitivity limit (–42 dBm) and consequently, the OSC optical link can be rebuilt, allowing the restoration of the Section DCC (SDCC) or multiplex section DCC (MS-DCC). The network view for this condition is shown in Figure 1-27.

Figure 1-27   *Network View for Span Loss Change > 5 dBm and OSC Power Value at Receiver > –42 dBm*
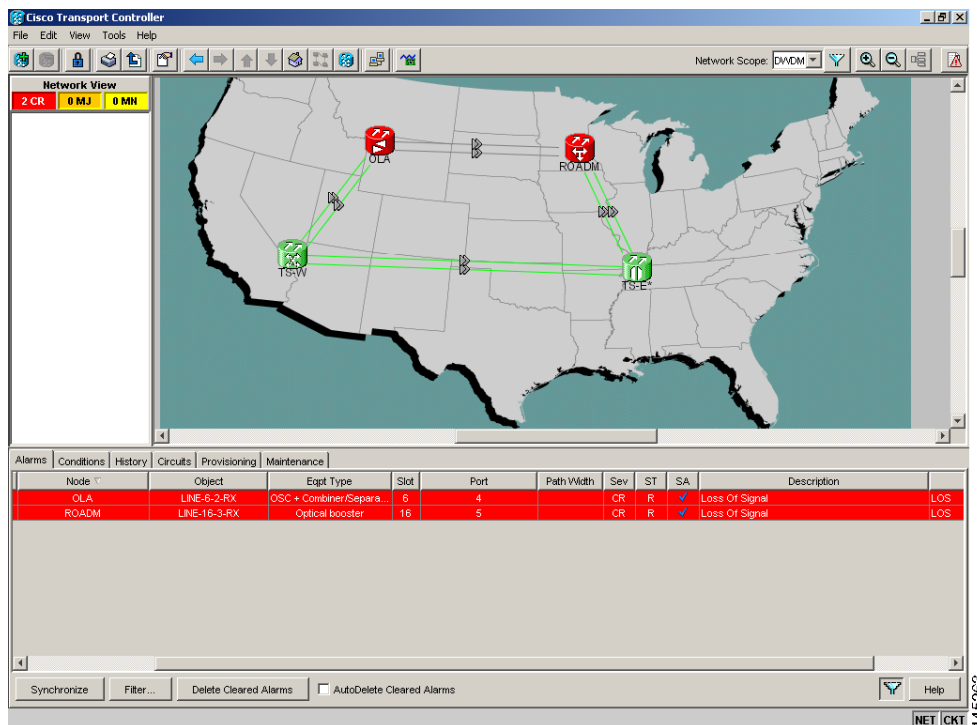
In node view, the EOC condition is cleared, but the alarm panels of the two nodes (ROADM and OLA in the example) continue to show LOS (OTS or AOTS) on the LINE-RX port of the OPT-BST or OSC-CSM.

The network ALS protocol keeps the OCHNC traffic down along the span because the new losses of the restored span can potentially affect the optical validation of the network design done by Cisco MetroPlanner.

Corrective Action for Scenario 2

Step 1   Verify the validity of the alarm. For both DWDM nodes connected to the repaired span:

    a.   Double-click the card directly connected with the span (either the OPT-BST or the OSC-CSM).

    b.   Click **Alarms**

    c.   Click the **Synchronize** button on the bottom left of the window.

    d.   Verify that a LOS condition is present on the LINE-RX port.

    e.   If the alarm is correctly reported, move to Step 3. If not, close the CTC application, delete the CTC cache, and open the CTC connection again. Then, go back to substep a.

> **Note**   If the "gray condition" of the span persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 2   Repair the fiber.

Step 3   Repair the fiber then measure the new Span Loss value.

    a.   In the node view of both nodes for the span, click the **Maintenance > DWDM > WDM Span Chec**k tabs.

    b.   Click **Retrieve Span Loss Values** to retrieve the latest loss data.

> **Note**   The two values retrieved at each node level (west side and east side) refer to the two fibers coming into the node from the adjacent nodes, so they apply to different spans. To complete the measurement in Step 3, the appropriate values must be taken into account.

Step 4   Compare the span measurements of Step 3 with the span losses values used during the network design with Cisco MetroPlanner.

Step 5   For the two fibers belonging to the repaired span, identify the fiber for the W–E line direction and calculate the insertion loss variation. If the span loss change is greater than 3 dBm, continue with Step 6. If not, go to Step 9.

Step 6   Clean the LINE-RX and LINE-TX connectors on the DWDM cards managing the fiber of the repaired span. If the problem persists, continue with Step 7.

Step 7   If the alarm condition is still reported, it is recommended that the fiber be repaired again to reestablish the expected span loss value. If this is not possible and the new value of span loss cannot be modified, go to Step 8 to fix the system faulty condition.

Step 8   Follow the signal flow into the network starting from the repaired fiber:

    a.   In the downstream node, identify the OPT-BST or OSC-CSM card that manages OSC and CHS detection.

    b.   In card view, click the **Provisioning > Optical Line > Optic Thresholds** tabs.

    c.   Click the **Alarms** radio button, then click **Refresh**.

    d.   Decrease the current OSC and CHS Fail Low thresholds by the same amount of the span loss change calculated in Step 5.

        If an OPT-BST is present:

        –   CHS Fail Low threshold refers to Port 2.

- OSC Fail Low threshold refers to Port 4.

If an OSC-CSM is present:

- CHS Fail Low threshold refers to Port 3.

- OSC Fail Low threshold refers to Port 6.

Step 9 For the two fibers belonging to the repaired span, identify the fiber for the east to west (E–W) line direction.

Step 10 Repeat the procedure from Step 5 to Step 8 for the E–W direction.

Step 11 If the LOS alarm has cleared, the system has restarted properly. However, because a span loss value significantly different is now present, we highly recommended that you complete the following procedure:

  a. Go back to the Cisco MetroPlanner tool and open the network design configuration file.

  b. Select **Installation Mode** to freeze the node layout and amplifier positioning.

  c. Change the span value, inserting the new span loss that was measured in Step 3.

  d. Run the Cisco MetroPlanner algorithm to validate the new design.

  e. If the optical result indications (power, optical signal-to-noise ratio [OSNR], chromatic dispersion [CD], and so on) are all green, the repair procedure is complete. If not, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

If the LOS alarm is still present, continue with Step 12.

Step 12 Go back to the card where the LOS alarm is active, and set the Optics Thresholds (see Step 8b) to the lowest value allowed.

If an OPT-BST is present:

- CHS Fail Low threshold must to be set to –30 dBm.

- OSC Fail Low threshold must to be set to –42 dBm.

If an OSC-CSM is present:

- CHS Fail Low threshold must to be set to –30 dBm.

- OSC Fail Low threshold must to be set to –40 dBm.

Note If the LOS alarm is still present, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 13 If the LOS alarm is has cleared, the system has restarted properly, but because a Span Loss value significantly different from the design is now present, we highly recommend that you complete the procedure described in Step 11.

1.12.2.3 Scenario 3: 3 dBm < Span Loss Change < 5 dBm

In network view, both the lines representing the span change to green after the rebuild of the OSC optical link and consequent restoration of the SDCC or MS-DCC. The EOC condition and the LOS alarms are cleared.

The network ALS protocol successfully restarts the amplifiers, which enables the OCHNC traffic restoration along the span.

The reactivation of the OCHNC circuits relating to the repaired span (the status changes from Partial to Complete) can lead to several final conditions that depend on the network topology and node layout.

The rebuilding of circuits automatically triggers the APC check mechanism (for details, refer to the "Automatic Power Control" section in the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*). The APC check mechanism impacts the optical gain of the amplifiers (primarily the OPT-PRE card) and the VOA express attenuation for the optical add/drop multiplexing (OADM) cards. The APC application acts on the appropriate cards downstream of the repaired span (for each line direction), and attempts to compensate for the introduction of excess loss.

Because the loss increase exceeds the maximum variation (+/–3 dBm) for which APC is allowed to compensate, an APC-CORRECTION-SKIPPED condition is raised by the first node along the flow detecting the event. The condition panel of the impacted node (the ROADM, in this example) reports the APC-CORRECTION-SKIPPED condition and indicates the port or card to which it applies.

To correct Scenario 3:

Step 1   Verify the alarm validity. For both DWDM nodes connected to the repaired span:

    a.   Double-click the card reporting the issue.

    b.   Click **Conditions**.

    c.   Click **Retrieve** and verify that an APC-CORRECTION-SKIPPED condition is present on an aggregate port.

    d.   If the alarm is correctly reported, go to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again. Then, go to substep a.

> ✎
> **Note**   If the discrepancy persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 2   Repair the fiber and measure the new Span Loss value after the fiber has been repaired.

    a.   In the node view of both nodes of the span, click the **Maintenance > DWDM > WDM Span Check** tabs.

    b.   Click **Retrieve Span Loss Values** to retrieve the latest loss data.

> ✎
> **Note**   The two values retrieved at each node level (west side and east side) refer to the two fibers coming into the node from the adjacent nodes, so they apply to different spans. To complete the measurement in Step 3, the appropriate values must be taken into account.

Step 3   Compare the span measurements of the previous step with the Span Losses values used during the network design with Cisco MetroPlanner.

Step 4   For the two fibers belonging to the repaired span, identify the one for the W–E line direction. If the span loss change is greater than 3 dB, continue with Step 5. If not, go to Step 8.

Step 5   Clean the LINE-RX and LINE-TX connectors of the DWDM cards that manage the fiber of the repaired span. If the problem persists, continue with Step 6. Otherwise, you are finished with the corrective action.

Step 6   If the alarm condition is still reported, we recommend that you again repair the fiber to reestablish the expected span loss value. If this is not possible and the new value of Span Loss cannot be modified, move to Step 7 to fix the system faulty condition.

Step 7   Follow the signal flow into the network starting from the repaired fiber.

a.   In the first downstream node of the restored span (W–E), check whether a DWDM card reports the APC-CORRECTION-SKIPPED condition on a port applying to the W–E direction (see Step 2 for directions to do this).

b.   If the answer is yes, retrieve the following values according to the card type.

- For OPT-PRE or OPT-BST cards: Click the **Provisioning > Optical Ampli. Line > Gain Setpoint** tabs

- For AD-xC-xx.x or AD-xB-xx.x cards: Click the **Provisioning > Optical Line > VOA Attenuation Reference** tabs.

- Go to Step 7f.

c.   If the answer is no, go to Step 7d.

d.   Move along the downstream nodes until a card with the APC-CORRECTION-SKIPPED condition for a W–E port is detected.

e.   From that card, retrieve parameters according to Step 7b.

f.   In the first downstream node of the restored span, go to the Circuits tab and identify all the OCHNC circuits passing through the repaired span.

g.   Edit all the OCHNC circuits identified in Step 7f:

- Click the **Tools > Circuits > Set Circuit State** tabs.

- Change the Target Circuit Admin. State to **OOS DSBLD** (or, **locked, disabled**) and click **Apply**.

h.   Go to the DWDM card for which the Gain or VOA Attenuation values were retrieved (the card can be either the one in substep Step 7b or Step 7e) and verify that the administrative state of the alarmed port is now OOS (locked).

i.   If the alarmed port is not OOS (locked), go to the card view, click **Circuits**, and identify the remaining OCHNC circuits that are still active. Put the circuits in **OOS DSBLD** (or, **locked, disabled**) in order to reach the OOS (locked) administrative state on the alarmed port.

j.   Wait for three minutes, then switch the administrative state of only one of the circuits selected in Step 7f and Step 7i back to **IS**, (unlocked).

k.   After the network completes the restart phase, go to the formerly alarmed card and verify that the APC-CORRECTION-SKIPPED condition has cleared and a new Gain Setpoint or VOA Attenuation Reference (compare with Step 7b) has been provisioned.

✎ **Note**   The total variation of the above Gain Setpoint or VOA Attenuation Reference setpoint must be within approximately +/– 1 dBm of the Span Loss value measured in Step 2.

l.   If the APC-CORRECTION-SKIPPED condition has cleared and the system has restarted properly, we highly recommend that you complete the following procedure due to the fact that a Span Loss value that is significantly different than the design is now present.

- Go back to the Cisco MetroPlanner tool and open the network design configuration file.

- Select Installation Mode to freeze the node layout and amplifier positioning.

- Change the span value, inserting the new Span Loss measured in Step 2.

– Run the Cisco MetroPlanner algorithm to validate the new design.

– If the optical result indications (power, OSNR, CD, and so on) are all green, the repair procedure is complete. If not, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Note   If the APC condition persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 8   For the two fibers belonging to the repaired span, identify the fiber for to the east to west (E–W) line direction.

Step 9   Repeat the procedures from Step 5 to Step 7 for the E–W direction.

1.12.2.4 Scenario 4: Span Loss Change < 3 dB

In network view, both the lines that represent the span turn green after the rebuilding of the OSC optical link and consequent restoration of the SDCC or MS-DCC. The EOC condition and LOS alarms are cleared.

The network ALS protocol successfully completes the amplifier restart to enable OCHNC traffic restoration along the span.

The rebuilding of circuits automatically triggers the APC check mechanism (for details, refer to the "Automatic Power Control" section in the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*). The APC check mechanism affects the optical gain of the amplifiers (primarily the OPT-PRE) and the VOA express attenuation for the OADM cards. The APC application acts on the "suitable" cards downstream of the repaired span (for each line direction), and attempts to compensate for the introduction of excess loss.

The APC operation is successfully completed if enough margin during the Cisco MetroPlanner network design phase has been taken into account. If not, the adjustment done by the APC application overcomes the range setting for a specific optical parameter in the first appropriate card along the flow and an APC-OUT-OF-RANGE condition is raised. The condition panel of the impacted node (the ROADM in the example) reports the APC-OUT-OF-RANGE condition and indicates the port or card to which it applies.

To correct Scenario 4:

Step 1   Verify the alarm validity. For both DWDM nodes on the repaired span:

a.   Double-click the card reporting the issue.

b.   Click **Conditions**.

c.   Click **Retrieve** and verify that an APC-OUT-OF-RANGE condition is present on an aggregate port.

d.   If the alarm is correctly reported, go to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again. Then, go to Step 1.

Note   If the discrepancy persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 2 Repair the fiber and measure the new Span Loss value.

    a. In the node view of both nodes for to the span, click the **Maintenance > DWDM > WDM Span Check** tabs.

    b. Click **Retrieve Span Loss Values** to retrieve the latest loss data.

Note The two values retrieved at each node level (west side and east side) refer to the two fibers coming into the node from the adjacent nodes, so they apply to different spans. To complete the measurement in Step 3, the appropriate values must be taken into account.

Step 3 Compare the span measurements done in Step 2 with the Span Losses values used during the network design with Cisco MetroPlanner.

Step 4 For the two fibers belonging to the repaired span, identify the one for the W–E line direction.

- If the span loss change is greater than 1 dBm, continue with Step 5.
- If the span loss change is 1 dBm or less, move to Step 8.

Step 5 Clean the LINE-RX and LINE-TX connectors of the DWDM cards that manage the fiber of the repaired span.

Step 6 If the problem persists, continue with the next step. if not, you have finished the corrective action.

Step 7 if the span loss change is greater than 1 dBm and the APC-OUT-OF-RANGE condition still exists, it is mandatory to again repair the fibers to reestablish the expected span loss value.

Note If it is not possible to reduce the span loss change to under 1 dBm through fiber repair, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem

Step 8 For the two fibers belonging to the repaired span, identify the fiber for the east to west (E–W) line direction.

Step 9 Repeat the procedure from Step 5 to Step 7 for the E–W direction.

1.12.3 OCHNC Circuits Creation Failure

OCHNC circuit creation is managed by the Cisco Wavelength Path Provisioning (WPP) network application. The WPP application helps prevent errors during new circuit activation (if the wavelength is already allocated in the path between source and destination) and also guarantees an appropriate time interval between one circuit activation and the next to enable proper amplifier gain regulation by APC.

WPP uses the network topology information carried by the OSC link among different nodes to identify the routing path of the optical wavelength (OCHNC circuits) from the source node to the destination node. WPP also enables the card ports of the OCHNC circuits by changing the administrative state from the default Out Of Service (OOS, or locked) state to the final In Service (IS), or unlocked state.

1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation

The prerequisite conditions for successfully completed circuit creation are:

1. Internode: OSC link active among all DWDM nodes involved

2. Internode: APC enabled (or alternatively manually disabled by the user)

3. Intranode: Logical connections among cards created and provisioned on every node of the network (ANS completed)

OCHNC circuit creation is successfully completed when the CTC circuit table reports the situation shown in Figure 1-28.

- Circuit Status has turned to DISCOVERED.

- The # of spans field shows the correct number of hops among different nodes that the OCHNC circuit passes through to reach the final destination.

- Circuit State reports IS (unlocked).

Figure 1-28   OCHNC Circuit Successfully Completed
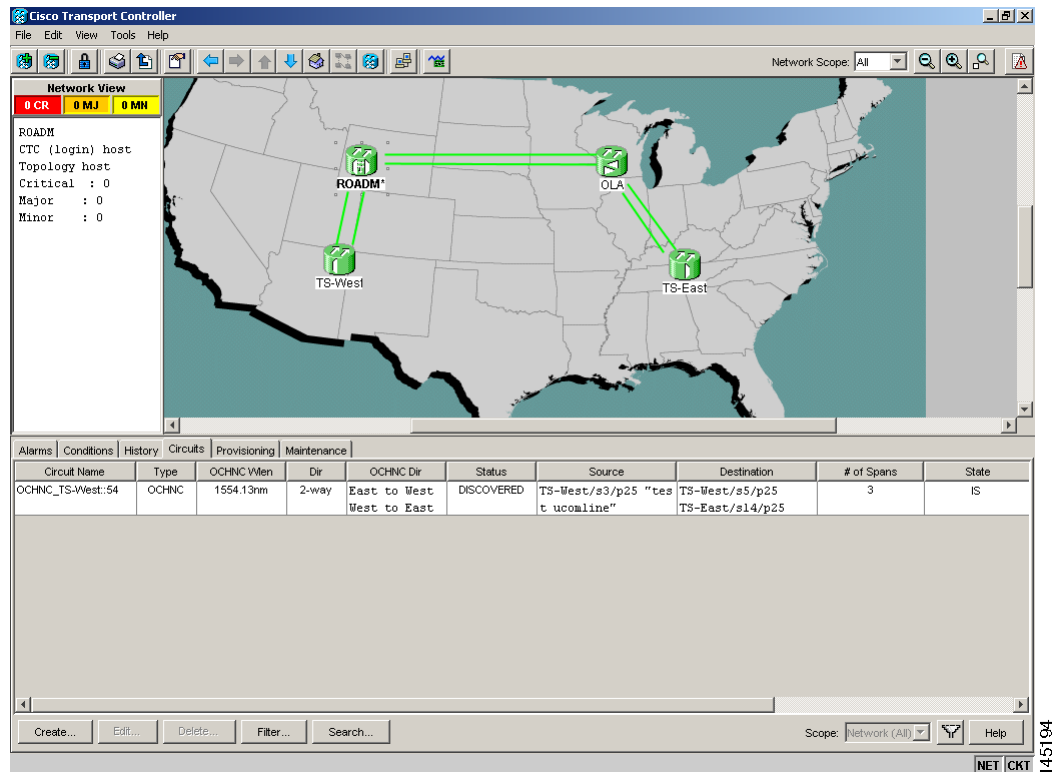
1.12.3.2 Conditions for OCHNC Circuit Creation Failure

If the OCHNC circuit creation fails, you will see one of the following conditions.

- If the WPP wizard cannot complete the circuit creation procedure, CTC displays the error message shown in Figure 1-29. In the message, click **Details** to see the partial connections that WPP can set up.Start troubleshooting the problem in the first node unreachable along the path.

Figure 1-29   Partial Circuit
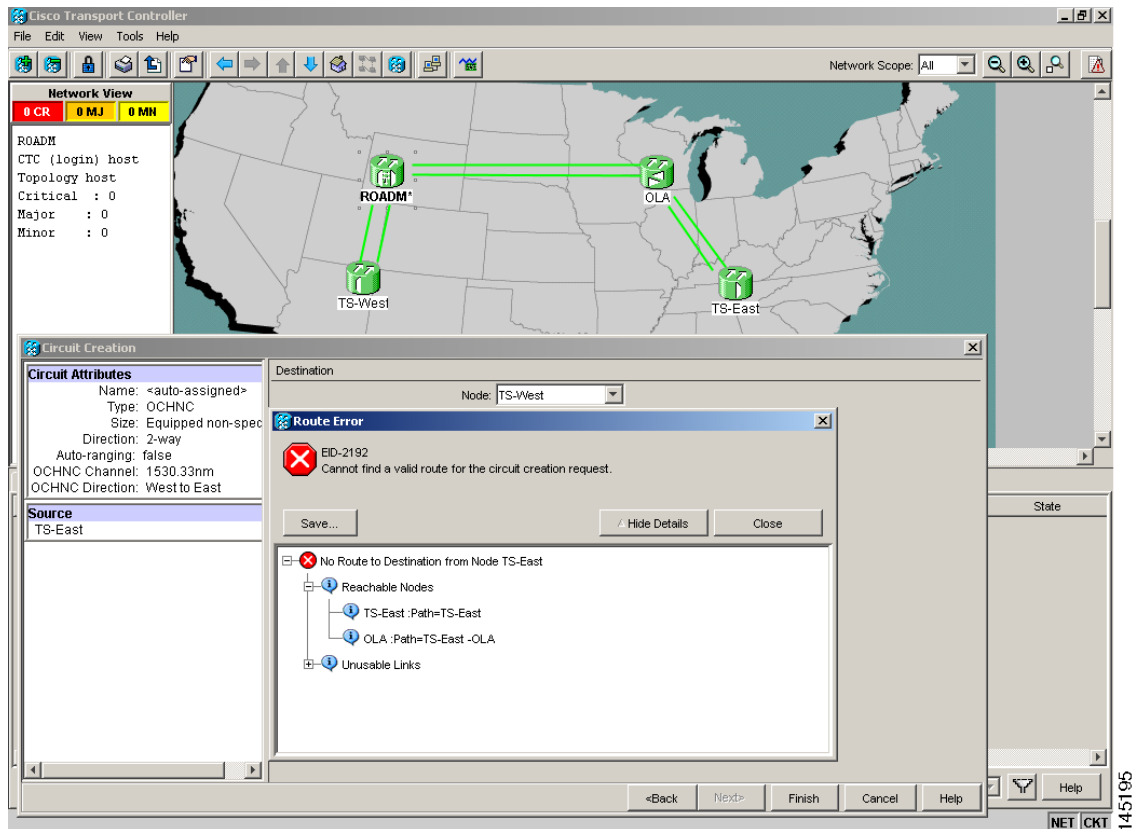
- The circuit is successfully created and reported under the Circuits tab, the Status field turns to DISCOVERED, but the Circuit State is OOS (locked). The condition is shown in Figure 1-30.

Figure 1-30   Circuit Discovered, State OSS
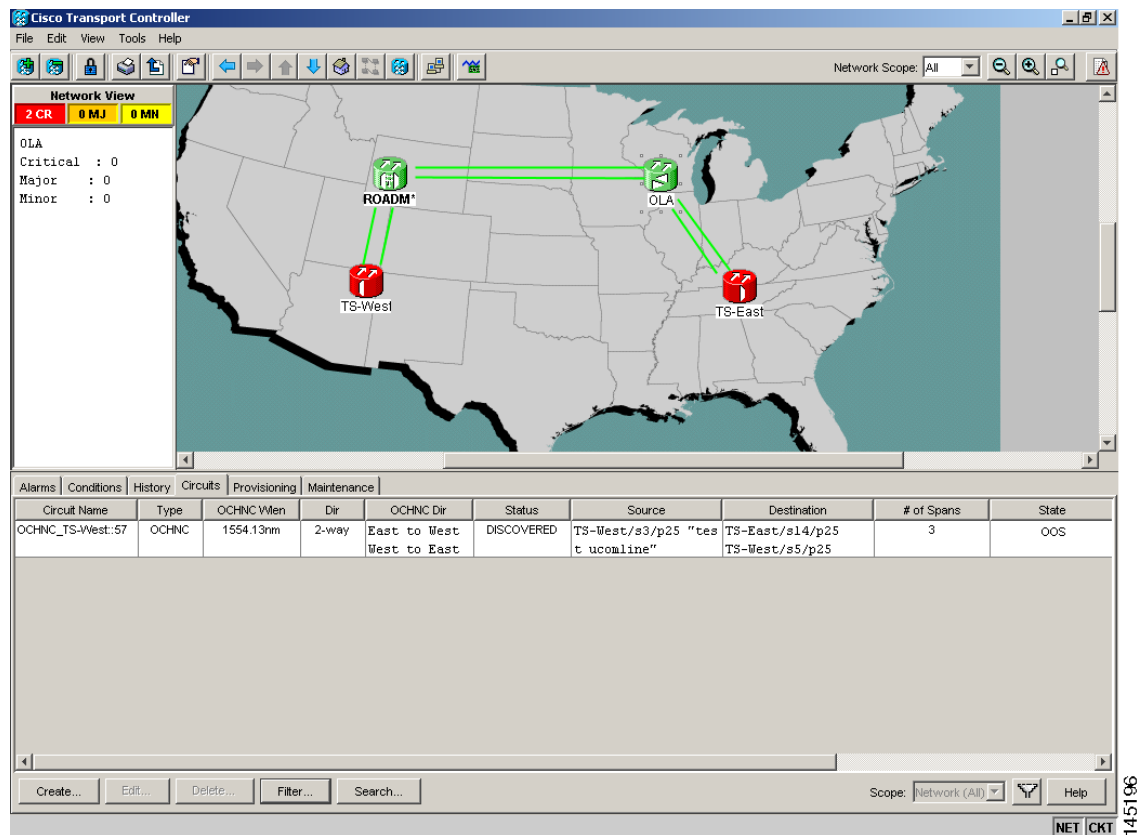
- The OCHNC circuit is shown under the Circuits tab, but the Status field reports PARTIAL. This applies to a circuit successfully built-up when the network falls into scenarios 1. (OSC link fail) or 2. (APC disabled), described in "1.12.3.3 Scenarios for OCHNC Circuit Creation Failure" section on page 1-77.

The root cause identification for the preceding conditions are found in the prerequisite conditions described in "1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation" section on page 1-74.

1.12.3.3 Scenarios for OCHNC Circuit Creation Failure

The most common scenarios for failure to create an OCHNC circuit are:

1. One (or more) of the span OSC links involving the OCHNC circuit has not been properly established. The WPP application prevents the creation of any circuit passing through the failing span. Prerequisite condition 1. of "1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation" section on page 1-74 has not been met.

2. The APC application is internally disabled due to the presence of a Critical alarm somewhere in the network. As a consequence, no reliable information about the number of active channels can be shared among the nodes and the creation of any further OCHNC circuit is prevented until the faulty condition is fixed. Prerequisite condition 2. of "1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation" section on page 1-74 has not been met.

3. One (or more) of the intranode connections between two DWDM cards associated with the circuit have not been properly created. Prerequisite condition 3. of 1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation has not been met.

4. One (or more) of the intranode connections between two DWDM cards associated with the circuit has not been properly provisioned. This happens when ANS application has not run in one of the involved nodes or at least one port status after the ANS run has not been successfully configured (Fail-Out of Range alarm on the ANS panel). Prerequisite condition 3. of 1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation has not been met.

To troubleshoot and eventually fix issues related to the faulty OCHNC circuit creation shown in Figure 1-29, the following procedure must be performed.

Step 1   Verify OSC connectivity:

a. Go to network view and identify the MSTP nodes to which the OCHNC circuit applies.

b. Verify that all the OSC links connecting the MSTP nodes along the circuit path, from the source node to the destination node, are active (green line).

> ✎
> **Note**   Bidirectional circuits have two possible nodes, depending on the line direction being considered.

Complete one of the following actions depending on OSC connectivity:

- If the OSC link is down, focus on the affected span and troubleshoot the issue (see 1.12.2 System Restart after a Fiber Cut, page 1-65).

> ✎
> **Note**   If necessary, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

- If the OSC link is not down, continue with Step 2.

Step 2   Verify APC status:

a. Go to node view on the MSTP node that is the source node for the circuit.

b. In the General Info box on the left, check the APC state (last row).

- If the APC state is DISABLE - INTERNAL, choose the appropriate troubleshooting procedure according to Chapter 2, "Alarm Troubleshooting" of the *DWDM Alarm and Troubleshooting Guide*.

> ✎
> **Note**   If necessary, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

- If the APC state is not DISABLE - INTERNAL, continue with Step 3.

Step 3   Verify that the intranode connections have been built in:

a. Go to the node view on the MSTP node that is the source node for the circuit.

b. Click the **Provisioning > WDM-ANS > Connections** tabs.

c. Verify the all node connections have been created and that their state is Connected.

> **Tip**   To quickly verify the connections, click the **Calculate Connection** button and check to see if any new connections come up.

If some connections are missing, perform the proper procedure according to Chapter 3, "Turn Up a Node" in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 4   If necessary, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

1.13 Node Level (Intranode) Problems

Troubleshooting for node-level optical channel (OCH) VOA start-up failure is discussed in this section.

> **Note**   In the following paragraphs, a reference to the 32-WSS card also includes the 32-WSS-L card.

A dedicated VOA regulates the optical power for every single channel (single wavelength) inserted in the MSTP system through a 32-WSS, 32MUX-O, or AD-xC-xx.x card.

The final state for the VOAs is the power control working mode. In this mode, the attenuation that the VOA introduces is automatically set based on the feedback provided from a dedicated photodiode, so that a specific power setpoint value is reached and maintained.

Prior to following the procedures in this section, pay attention to the following information.

> **Note**   The ALS function should only be disabled temporarily for installation or maintenance reasons. Activate ALS immediately after maintenance or installation.

The following warning applies to handling unterminated fibers when ALS is disabled:

> **Warning**   **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

1.13.1 VOA Startup Phases

The final VOA condition is achieved through a startup procedure divided into the four sequential phases shown in Figure 1-31.

Figure 1-31   VOA Startup Procedure
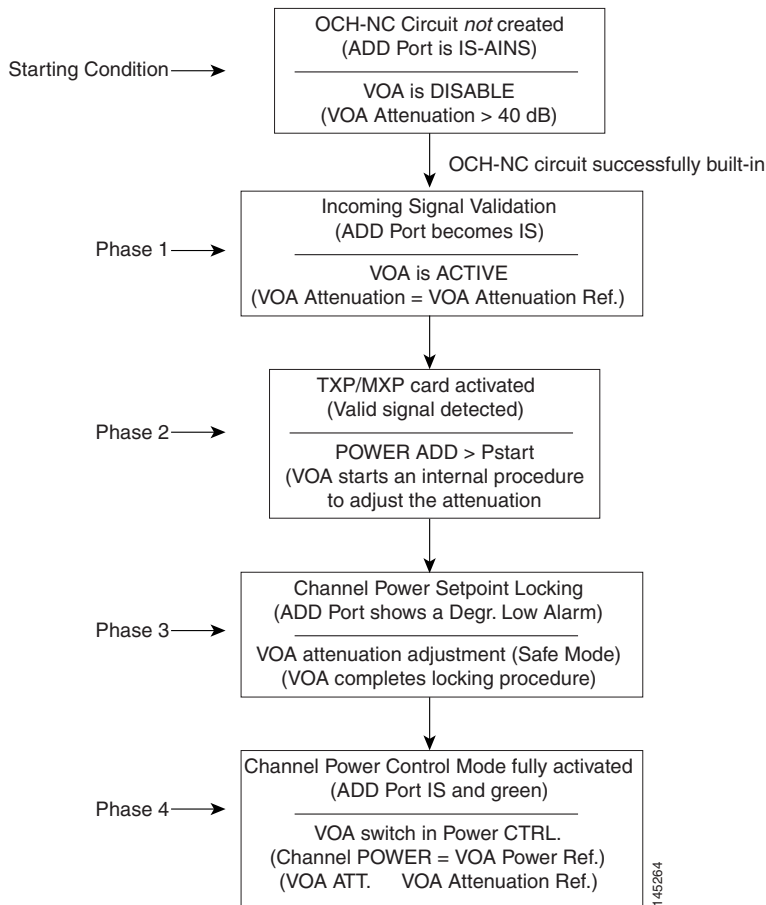
Until the VOA has completed all the phases shown in Figure 1-31, the power control mode is not fully activated.

1.13.1.1 Phase 1: Incoming Signal Validation

The Incoming Signal Validation phase checks to see that the optical interface connection is valid and that the optical power level is appropriate.

Cisco MetroPlanner calculates the VOA Attenuation Reference value to allow only supported MSTP interfaces to overcome the power start-up (Pstart-up) acceptance level. (Refer to the "Network-Level Gain—Tilt Management of Optical Amplifiers" section in the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.).

If the interface that is connected has a power value outside the allowed range, the Phase 1 check prevents OCHNC turn-up.

1.13.1.2 Phase 2: TXP/MXP Card Activated (Valid Signal Detected)

If Phase 1 indicates that the signal is valid, an automatic iterative attenuation adjustment on the VOA takes place to reach a power target on the photodiode downstream of the VOA.

Note   The power setpoint is generated by Cisco MetroPlanner on a case-by-case basis. During the ANS run, the power target is provisioned on the VOA.

1.13.1.3 Phase 3: Channel Power Setpoint Locking

In Phase 3, the VOA is kept in a transient standby condition when a steady power value close enough to the final power setpoint has been reached (nominally 3 dBm lower).

The duration of the transient standby condition is three seconds (by default) and allows safe management of optical interfaces that have different signal rise time values or are undergoing a pulse startup procedure compliant with the ITU-T G664 recommendation.

1.13.1.4 Phase 4: Channel Power Control Mode Fully Activated

The VOA reaches the final attenuation condition that leads the power value that is read on the photodiode to the expected target value (VOA Power Reference). Simultaneously, the VOA operating mode switches to power control mode.

From this point on, any further adjustment of the VOA attenuation is triggered by a variation of the value read on the photodiode. The aim of these adjustments is to always keep the power value equal to the power setpoint, with +/– 0.5 dBm as the minimum adjustment increment.

1.13.2 VOA Failure Scenarios

Several conditions can stop the startup procedure at an intermediate step, blocking the VOA (and the circuit activation, as a consequence) from completing activation of the power control mode. The scenarios in this section portray those conditions.

Root-cause identification can be performed based on the alarm raised and the power reading on the photodiode associated with the VOA.

1.13.2.1 Scenario A: Optical Power Level of the Incoming Signal Lower Than Minimum Allowed by MSTP Supported Optical Interfaces

This scenario is for a condition where a TXP or MXP card is directly connected to a 32MUX-O or 32WSS card where power in is expressed as Pin < – 4.5 dBm.

If the incoming power level is lower than the minimum allowed, the startup procedure always stops at Phase 1 (see Figure 1-32). This is the case even if the final VOA Power Reference reported in CTC is reachable.

The final conditions that CTC reports are:

- A LOS-P (OCH layer) alarm on the port associated with the VOA (see Figure 1-32)
- A valid (different from the end of scale value of – 50 dBm) optical power value in the Power field, but the value for Power is less than – 33 dBm. (To view the Power field, in card view, click the **Provisioning > Parameters** tabs.)

Figure 1-32   LOS-P Indication on the VOA Port
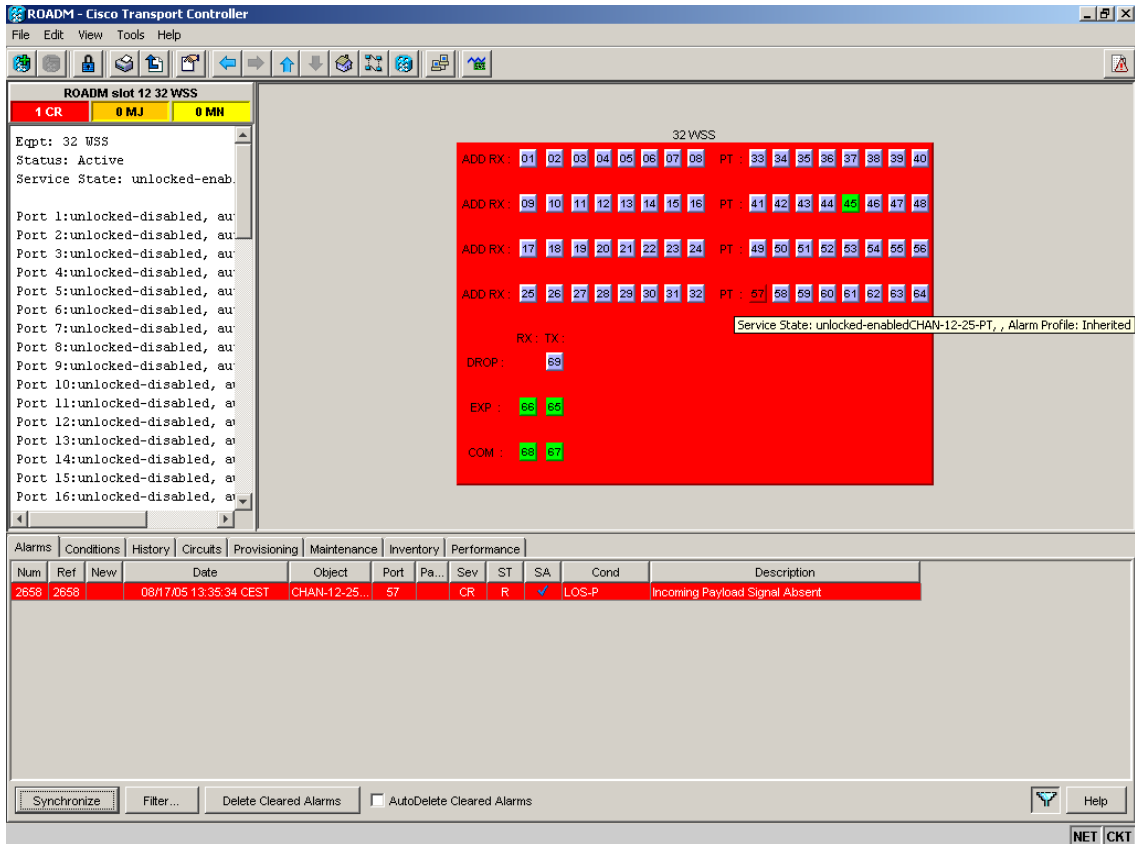
Use the following procedure to troubleshoot and eventually fix issues related to the VOA start-up when the optical power level of the incoming signal is lower than the minimum allowed by the MSTP supported optical interfaces (32MUX-O and 32WSS cards).

Step 1   Verify the alarm validity:

a. Identify the DWDM nodes where the alarmed card is seated.

b. Double-click the card (either the 32MUX-O or the 32WSS card).

c. Click **Alarms**.

d. Verify that a LOS-P alarm is present on the ADD-RX port.

e. Click the **Synchronize** button in the bottom left of the window.

f. If the alarm is correctly reported, move to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again.

Note   If the alarm inconsistency persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 2   f the alarmed card is a 32WSS, verify the incoming power level from the connected TXP, MXP, or line card. If the alarmed card is a 32MUX-O, go to Step 5.

a. Double-click the 32WSS card.

b. Click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs to display the optical power physically coming into the 32WSS ADD-RX port.

> **Note**   X is the number (1 to 4) of the appropriate multifiber push-on (MPO) connector that manages the alarmed channel (wavelength).

c. Identify the proper channel (wavelength) and read the Power ADD field.

d. If the Power ADD value is less than –4.5 dBm, go to Step 3. If not, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

> **Note**   X is the number (1 to 4) of the appropriate multifiber MPO connector that manages the alarmed channel (wavelength).

e. Identify the correct row based on the **Type** field (the row must indicate Add in the type field).

f. Decrease the attenuation on the VOA to the minimum (0 dB) to enable channel startup. To perform this adjustment:

   • Read the VOA Attenuation Ref value for the channel (wavelength).

   • Enter into the VOA Attenuation Calib field the same value as that of the VOA Attenuation Ref field, but with the opposite sign (the algebraic sum of the two contributions must be equal to zero).

   • Click **Apply**. If the LOS-P alarm persists, continue with this procedure. Otherwise, the problem has been corrected.

g. In card view, click **Circuits**.

h. Delete the OCHNC circuit that relates to the faulty channel.

i. Ensure that the corresponding ADD-RX service state port changes to **IS-AINS** (or unlocked, automaticInService) and that the color changes to grey (the LOS-P alarm should clear).

j. Recreate the OCHNC circuit and verify that the Status field reports DISCOVERED and that the state is IS (unlocked).

k. If the LOS-P alarm has not cleared, replace the 32WSS card (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*). Before you replace the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 3   Because the actual power received by the 32WSS card is lower than expected, verify the correct behavior of the TXP, MXP, or line card connected to the 32WSS:

a. The TX laser must be active (trunk port is in **IS** [or, **unlocked**] state).

b. The wavelength provisioned must be the proper one.

c. The output power value must be within the expected range (refer to the "Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

d. If the TX laser is active, the wavelength is provisioned properly, and the output power value is in the correct range, go to Step 4. Otherwise, take the appropriate corrective action, including card replacement if the output power value is outside of the expected range (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Replacing the card should correct the problem.)

Step 4 If the TXP or MXP card behaves as expected, the only remaining root-cause is the fiber connection between the two cards:

a. Verify that the ADD_RX port of the alarmed 32WSS is connected to the TRUNK_TX port of the TXP or MXP card using an MPO-LC multifiber cable.

> **Note** A patch-panel tray is normally used to manage fiber connections (for patch-panel cabling details, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*).

b. Check and clean the LC fiber fan-out according to site practice. The fiber numbers (1 to 8) must correspond to the wavelength managed.

c. If a patch panel is used, check and, if necessary, clean the LC-LC adapter. If necessary, replace any bad devices (maximum tolerance is 1 dB).

d. Pull out the LC connector from the TRUNK_TX port of the TXP or MXP card and clean the fiber according to site practice.

> **Note** If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

> **Note** If the alarm condition has not cleared, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 5 When the alarmed card is a 32MUX-O, the troubleshooting procedure should start from the TXP, MXP, or line card. Verify the correct behavior of the TXP, MXP, or line card connected to the 32MUX-O:

a. The TX laser must be active (trunk port is in **IS** [or unlocked] state).

b. The wavelength provisioned must be the proper one.

c. The output power value must be within the expected range (refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

d. If the TX laser is active, the wavelength is provisioned properly, and the output power value is in the correct range, go to Step 6. Otherwise, take the appropriate corrective action, including card replacement if the output power value is outside of the expected range (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Replacing the card should correct the problem.)

Step 6 If the TXP or MXP card behaves as expected, check the fiber connection between the two cards:

a. The ADD_RX port of the alarmed 32MUX-O must be connected to the TRUNK_TX port of a TXP or MXP card using an MPO-LC multifiber cable.

Note   A patch-panel tray is normally used to manage fiber connections (for patch-panel cabling details, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*).

b. Check and clean the LC fiber fan-out according to site practice. The fiber numbers (1 to 8) must correspond to the wavelength managed.

c. If a patch panel is used, check and, if necessary, clean the LC-LC adapter.

d. If necessary, replace any bad devices (maximum tolerance is 1 dB).

e. Pull out the LC connector from the TRUNK_TX port of the TXP or MXP card and clean the fiber according to site practice.

Note   If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

f. If the alarm condition persists, move to Step 7. Otherwise, the problem has been corrected.

Step 7   Verify the correct behavior of the VOA inside the 32MUX-O card:

a. Double-click the 32MUX-O card.

b. Click **Circuits**.

  • Delete the OCHNC circuit relating to the faulty channel.

  • Ensure that the service state of the corresponding ADD-RX port changes to IS-AINS (or unlocked, automaticInService), and that the color turns grey (the LOS-P alarm should clear).

c. In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs and identify the proper channel (wavelength).

Note   X refers to one of the 32-WSS connectors

d. Decrease the attenuation on the VOA to the minimum (0 dB) to enable channel startup. To perform this in field adjustment:

  • Read the VOA Attenuation Ref value for the channel (wavelength).

  • Enter the same value into the VOA Attenuation Calib field as that of the VOA Attenuation Ref field, but with the opposite sign (the algebraic sum of the two contributions must be equal to zero).

  • Click **Apply**. If the LOS-P alarm persists, continue with this procedure. Otherwise, the problem has been corrected.

e. Click **Circuits**.

f. Recreate the OCHNC circuit and verify that Circuit Status field reports DISCOVERED and the state is IS (unlocked).

g. If the LOS-P alarm has not cleared, replace the 32MUX-O card (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*). Before you replace the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem).

1.13.2.2 Scenario B: Optical Power Level of the Incoming Signal Lower Than Expected

In some cases, the pass-through channels on the 32WSS card or the optical bypass channels on the 32MUX-O card are at a power level that is lower than expected. The incoming power level can be lower than expected for several reasons. A few examples are:

- Dirty connections
- Excessive span loss
- Wrong amplifier gain setting

When the power is lower than expected, the start-up procedure can stop at Phase 1, Phase 2, or Phase 3 (see Figure 1-31). The point at which the start-up procedure stops depends on the amount of power missing.

Given that delta power is the amount of optical power missing compared to the expected value, two final conditions for Scenario B can be identified, conditions B1 and B2.

1.13.2.2.1 Condition B1—Delta Power > 6 dB (LOS-P Alarm)

When the optical power is greater than 6 dB lower than the expected value, the final VOA Power Reference setpoint value is definitively not reachable and even Phase 1 of the start-up procedure cannot be properly completed. As a consequence, the final condition reported in CTC is the same as that of Scenario A:

- A LOS-P (OCH layer) alarm is present on the port associated with the VOA.
- A valid (different from the end of scale value of – 50 dBm) optical power value can be read in the Power field, but the value for Power is less than – 33 dBm (see Figure 1-33). (To access this value, in card view, click the **Provisioning > Parameters** tabs.)

Figure 1-33   Power Level of Incoming Signal Less than –33 dBm
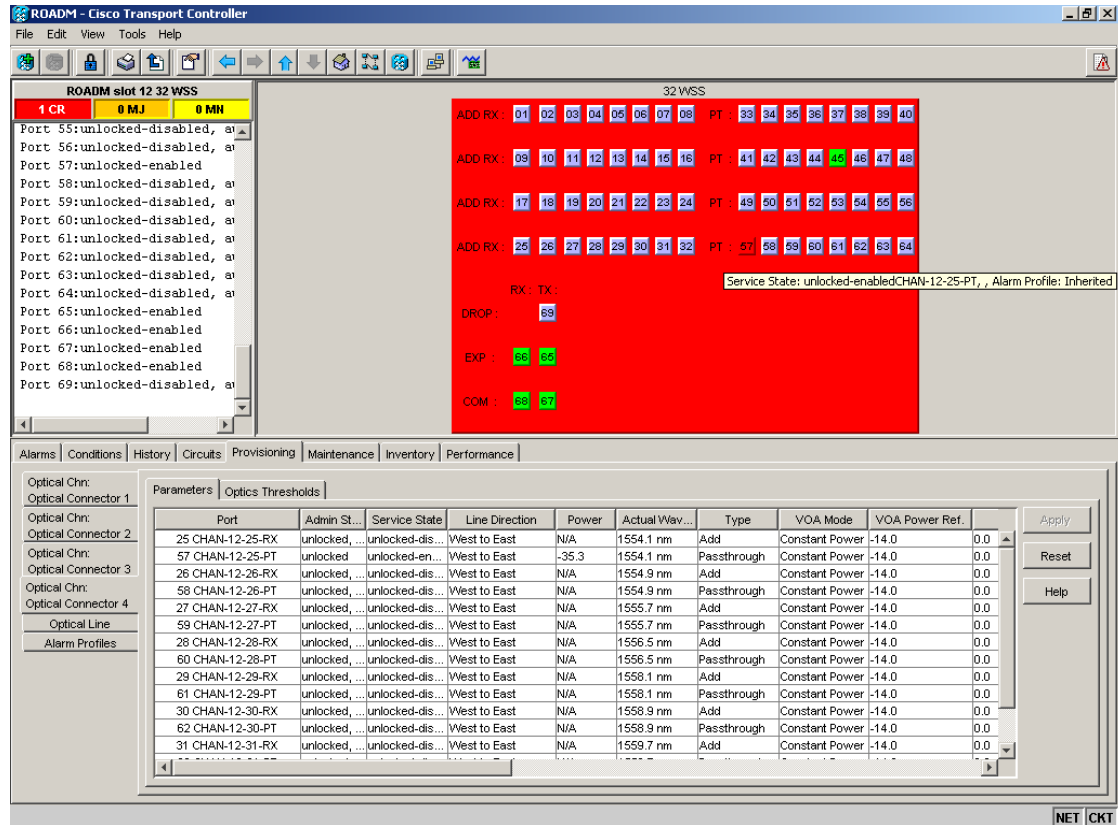
1.13.2.2.2 Condition B2—Delta Power < 6 dB (OPWR-LowDEGrade Alarm)

When the optical power is less than 6 dB lower than the expected value, even if a valid incoming signal is present, the final VOA Power Reference setpoint value that is reported in the CTC is not reachable and the VOA startup procedure is stopped at Phase 3.

The final conditions that CTC reports are:

- An OPWR-LowDEGrade (OCH layer) alarm is present on the port associated with the VOA.

- A valid (different from the end of scale value of –50 dBm) optical power value can be read in the Power field, but the value is (VOA Power Ref – 6 dBm) < Power < VOA Power Ref (see Figure 1-34). To access this value, in card view, click the **Provisioning > Parameters** tabs.

Figure 1-34   Optical Power Less than 6 dB Lower than Expected
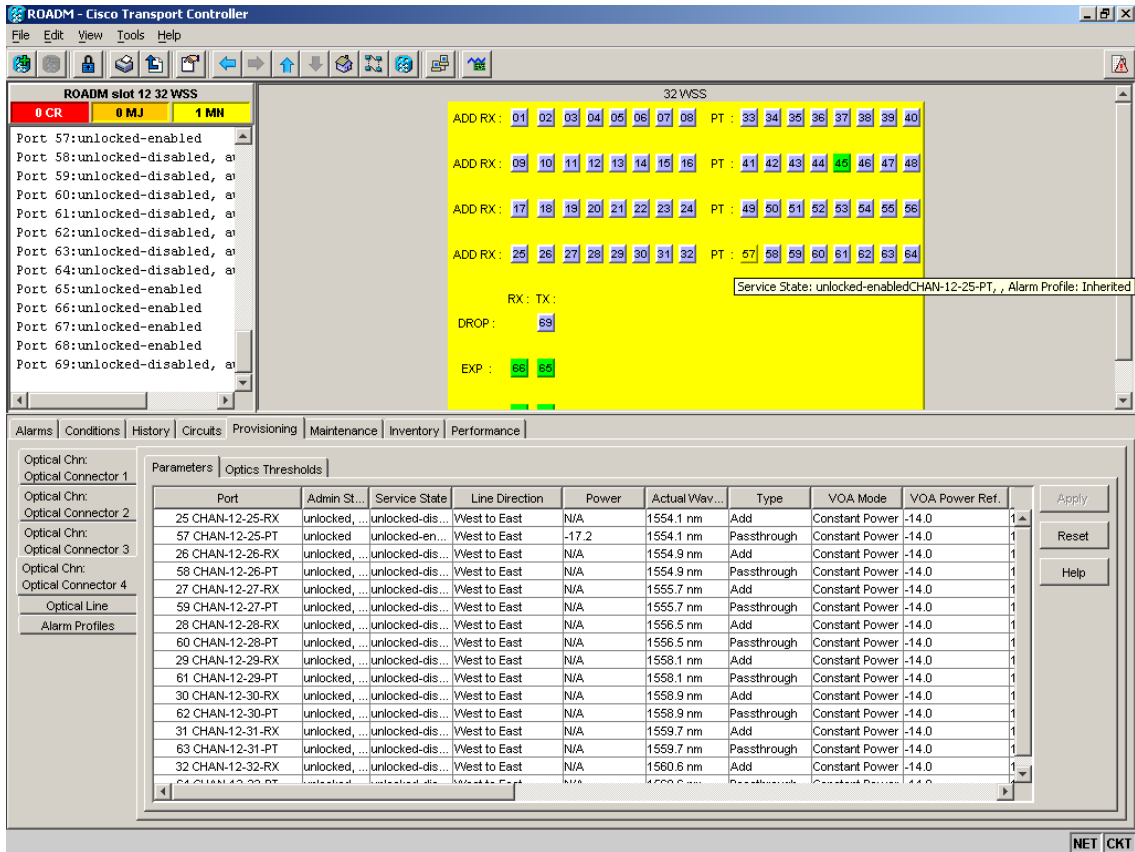
1.13.2.2.3 Corrective Actions for Scenario B (Optical Power Level of Incoming Signal Lower than Expected)

When the optical power level of the incoming signal is lower than expected for the pass-through channels on the 32WSS or the optical bypass channels on the 32MUX-O card, use the following procedure to troubleshoot and eventually fix issues related to VOA start-up:

According to the final conditions reported by the card (either LOS-P alarm for condition B1 or OPWR-LowDEGrade for condition B2), two troubleshooting procedures are suggested.

If condition B1 (see "1.13.2.2.1 Condition B1—Delta Power > 6 dB (LOS-P Alarm)" section on page 1-86) results in an LOS-P alarm, compete the following procedure:

Step 1 Verify the alarm validity:

    a. Identify the DWDM nodes where the alarmed card is located.

    b. Double-click the card (either the 32MUX-O or the 32WSS card).

    c. Click **Alarms**.

    d. Verify that a LOS-P alarm is present on the ADD-RX port.

    e. Click the **Synchronize** button at the bottom left of the window.

    f. If the alarm is correctly reported, move to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again.

> ✎
>
> **Note** If the alarm inconsistency persists, log into the Technical Support Website at
> http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in
> order to report a service-affecting problem.

Step 2 In card view, click **Circuits** and retrieve the node, card, and port information for the alarmed channel
from the Source field of the OCHNC circuit. Then follow the procedures of Step 3 (32MUX-O, 32WSS,
or AD-xC-xx.x card) or Step 4 (TXP, MXP, or line card) as appropriate.

Step 3 Verify the correct behavior of the far-end DWDM card (32MUX-O, 32WSS, or AD-xC-xx.x) that
manages the channel (wavelength):

a. Verify that the power value coming in on the ADD_RX port is correct.

 • In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

> ✎
>
> **Note** X is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed
> channel (wavelength).

 • The Power field value must be the same as that in the VOA Power Ref field. If not, take the
appropriate corrective actions according to the alarm raised at the RX-ADD port.

Step 4 Verify the correct behavior of the TXP, MXP, or line card that is the signal source of the channel
(wavelength) that is alarmed:

a. The TX laser must be active (trunk port is in IS [unlocked] state).

b. The wavelength provisioned must be the proper one.

c. The output power value must be within the expected range (refer to the "Hardware Specifications"
appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM
is not available through CTC (for example, TXP_MR_2.5G), perform a manual measurement using
a standard power meter.

Step 5 If the cards referenced in Step 3 and Step 4 are operating properly, go to Step 6. If not, take the
appropriate corrective actions according to the alarm raised on the card. See the appropriate procedure
for the alarm in Chapter 2, "Alarm Troubleshooting" of the *DWDM Alarm and Troubleshooting Guide*.

Step 6 If the alarmed card is a 32MUX-O, go to Step 9.

Step 7 If the alarmed card is a 32WSS, continue with the following steps:

a. Double-click the card.

b. Click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

> ✎
>
> **Note** X is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed
> channel (wavelength).

c. Identify the correct row based in the Type field (the row must indicate Passthrough in the type field).

d. Decrease the attenuation on the VOA to the minimum (0 dB) to enable channel startup. To perform
this in field adjustment:

 • Read the VOA Attenuation Ref value for the channel (wavelength).

 • Enter the same value into the VOA Attenuation Calib field as that of the VOA Attenuation Ref
field, but with the opposite sign (the algebraic sum of the two contributions must be equal to
zero).

- Click **Apply**. If the LOS-P alarm persists, continue with this procedure. Otherwise, the problem has been corrected.

  e. Click **Circuits**.

  f. Delete the OCHNC circuit for the faulty channel.

  g. Ensure that the service state of the corresponding ADD-RX port changes to IS-AINS (or unlocked, automaticInService) and that the color changes to grey (LOS-P alarm should clear).

  h. Recreate the OCHNC circuit and verify that Circuit Status field reports DISCOVERED and the state is IS (unlocked).

  i. If the LOS-P alarm has not cleared, continue with . Otherwise, the problem has been corrected.

Step 8   To unambiguously pinpoint the root cause of the alarm, verify the proper cabling of the EXP_RX port (which is the common input port for all the pass-through channels) on the 32WSS card:

  a. The EXP_RX port of the alarmed 32WSS must be connected to the EXP_TX port of the coupled 32WSS card on the opposite side of the node.

  b. Pull out the LC connector from the EXP_RX port of the 32WSS and clean the fiber according to site practice.

  c. Pull out the LC connector from the EXP_TX port of the coupled 32WSS and clean that connector also.

  d. Verify that the fiber attenuation is within the specifications (maximum tolerance is 1 dB).

  e. If necessary, replace any bad fibers.

> **Note**   If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

  f. If the alarm condition persists even after the checking and fixing the fibers, replace the 32WSS card (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*). Before replacing the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem).

Step 9   Verify the correct behavior of the VOA inside the 32MUX-O card:

  a. Double-click the 32MUX-O card.

  b. Click **Circuits**.

  c. Delete the OCHNC circuit for the faulty channel.

  d. Ensure that the service state of the corresponding ADD-RX port changes to IS-AINS (or unlocked, automaticInService) and that the color changes to grey (LOS-P alarm should clear).

  e. Click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs and identify the proper channel (wavelength).

> **Note** X is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

  f. Decrease the attenuation on the VOA to the minimum (0 dB) to enable channel startup. To perform this in field adjustment:

- Read the VOA Attenuation Ref value for the channel (wavelength).

- Enter the same value into the VOA Attenuation Calib field as that of the VOA Attenuation Ref field, but with the opposite sign (the algebraic sum of the two contributions must be equal to zero).

- Click the **Apply** button. If the LOS-P alarm persists, continue with this procedure. Otherwise, the problem has been corrected.

g. Click **Circuits**.

h. Recreate the OCHNC circuit and verify that Circuit Status field reports DISCOVERED and the state is IS (unlocked).

i. If the LOS-P alarm has not cleared, continue with Step 10. Otherwise, the problem has been corrected.

Step 10   To unambiguously pinpoint the root cause of the alarm, verify the proper cabling of the alarmed ADD_RX port on the 32MUX-O card:

a. The ADD_RX port of the alarmed 32MUX-O must be connected to the DROP_TX port of the coupled 32DMX-O card on the opposite side of the node using two MPO-LC multifiber cables.

> **Note**   A patch-panel tray is normally used to manage fiber connections (for patch-panel cabling details, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*).

b. Verify that the power value coming out of DROP_TX port of the coupled 32DMX-O card is correct:

- In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

  > **Note**   *X* is number (1 to 4) of the proper multi-fibers MPO connector that manages the alarmed channel (wavelength).

- The Power field value must be the same as that in the VOA Power Ref field. If it is not, take the appropriate corrective action for the alarm according to Chapter 2, "Alarm Troubleshooting.".

c. Check and clean the LC fiber fan-out according to site practice. The fiber numbers (1 to 8) must correspond to the wavelength managed.

d. Repeat Step c for the MPO-LC multifiber cable coming out of the DROP_TX port of the coupled 32DMX-O card.

e. Check and, if necessary, clean the LC-LC adapter.

f. If necessary, replace and bad devices (maximum tolerance is 1 dB).

> **Note**   If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

g. If the alarm condition persists even after the cabling is checked or fixed, replace the 32MUX-O card (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Before replacing the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem).

If condition B2 (see "1.13.2.2.2 Condition B2—Delta Power < 6 dB (OPWR-LowDEGrade Alarm)" section on page 1-87) results in an OPWR-LowDEGrade alarm, compete the following procedure:

Step 1 Verify the alarm validity:

   a. Identify the DWDM node where the alarmed card is located.

   b. Double-click the card (either the 32MUX-O or the 32WSS card).

   c. Click **Alarms**.

   d. Verify that an Optical Power Degrade Low (OPWR-LDEG) alarm is present on the ADD-RX port.

   e. Click the **Synchronize** button at the bottom left of the window.

   f. If the alarm is correctly reported, goto Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again.

> ✎ **Note** If the alarm inconsistency persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 2 In card view, click **Circuits** and retrieve the node, card, and port information for the alarmed channel from the Source field of the OCHNC circuit. Then, follow the procedures in Step 3 (for 32MUX-O, 32WSS, or AD-xC-xx.x cards) or Step 4 (for TXP, MXP, or line cards) as appropriate.

Step 3 Verify the correct behavior of the far-end DWDM card (32MUX-O, 32WSS, or AD-xC-xx.x) that manages the channel (wavelength). To do this, verify that the power value coming in on the ADD_RX port is correct:

   a. In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

> ✎ **Note** X is number (1 to 4) of the proper multi-fibers MPO connector that manages the alarmed channel (wavelength).

   b. The Power field value must be the same as that in the VOA Power Ref field. If it is not, take the appropriate corrective action for the alarm according to Chapter 2, "Alarm Troubleshooting" in the *DWDM Alarm and Troubleshooting Guide*.

Step 4 Verify the correct behavior of the TXP, MXP, or line card that is the signal source of the channel (wavelength) that is alarmed:

   a. The TX laser must be active (trunk port is in IS [unlocked] state).

   b. The wavelength provisioned must be the proper one.

   c. The output power value must be within the expected range (refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

Step 5 If the cards referenced in Step 3 and Step 4 are operating properly, go to Step 6. If not, take the appropriate corrective actions according to the alarm raised on the card (see Chapter 2, "Alarm Troubleshooting" in the *DWDM Alarm and Troubleshooting Guide)*.

Step 6 If the alarmed card is a 32MUX-O card, go to Step 8.

Step 7   If the alarmed card is a 32WSS card, verify the proper cabling of the EXP_RX port (common input port for all pass-through channels) on the 32WSS card:

    a. Verify that the EXP_RX port of the alarmed 32WSS is connected to the EXP_TX port of the coupled 32WSS card on the opposite side of the node.

    b. Pull out the LC connector from the EXP_RX port of the 32WSS card and clean the fiber according to site practice.

    c. Pull out the LC connector from the EXP_TX port of the coupled 32WSS card and clean its connector also.

    d. Verify that the fiber attenuation is within the specifications (maximum tolerance is 1 dB).

    e. If necessary, replace any bad fibers.

> **Note**   If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

> **Note**   If the alarm condition persists even after the cabling check/fixing, the root cause could be related to a network issue and a more accurate analysis of the signal flow is needed according to the actual system topology. If necessary, call Cisco TAC (1 800 553-2447) for help.

Step 8   Verify the proper cabling of the alarmed ADD_RX port on the 32MUX-O card:

    a. Verify that the ADD_RX port of the alarmed 32MUX-O is connected to the DROP_TX port of the coupled 32DMX-O card on the opposite side of the node, using two MPO-LC multifiber cables.

> **Note**   A patch-panel tray is normally used to manage fiber connections (for patch-panel cabling details, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*).

    b. Verify that the power value coming out of the DROP_TX port of the coupled 32DMX-O card is correct:

        • In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

> **Note** X is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

        • The Power field value must be the same as that in the VOA Power Ref field. If it is not, take the appropriate corrective action for the alarm according to Chapter 2, "Alarm Troubleshooting."

    c. Check (the number 1 to 8 must correspond with the wavelength managed) and clean the LC fan-out according to site practice.

    d. Repeat Step c for the MPO-LC multifiber cable coming out of the DROP_TX port of the coupled 32DMX-O card.

    e. Check and, if necessary, clean the LC-LC adapter used.

    f. If necessary, replace any bad devices (maximum tolerance is 1 dB).

> ✎
>
> **Note**   If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node." chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

> ✎
>
> **Note**   If the alarm condition persists even after the cable check and repair procedures, the root cause could be related to a network issue and a more accurate analysis of the signal flow is needed according with the actual system topology. If necessary, call Cisco TAC (1 800 553-2447) for help.

## 1.13.2.3 Scenario C: Optical Drop Power Level Lower Than Expected

This scenario describes the condition in which the optical power at the 32DMX-O drop channels is lower than expected. The 32DMX-O card is equipped with a VOA for each wavelength, and each VOA manages the power for one dropped wavelength.

The failing scenarios during the OCHNC turn-up and consequent VOA startup are the same as those described in the "1.13.2.2 Scenario B: Optical Power Level of the Incoming Signal Lower Than Expected" section on page 1-86. The only difference is the type of alarm that is raised when the condition exists in which delta power is greater than 6 dB.

1.13.2.3.1 Condition C1—Delta Power > 6 dB Lower than Expected

When the optical power on the dropped channel is greater than 6 dB lower that the value expected, the final VOA Power Reference setpoint value is definitively not reachable. As a consequence, the final conditions reported in CTC are as follows:

- An **OPWR-LFAIL** (OCH layer) alarm is present on the port associated with the VOA (see Figure 1-35).

- A valid (different from the end of scale value of – 50 dBm) optical power value can be read in the CTC Power field, but the Power value is less than – 33 dBm. (To view this value in card view, click the **Provisioning > Parameters** tabs.)

Figure 1-35   Optical Drop Power Greater than 6 dB Lower than Expected
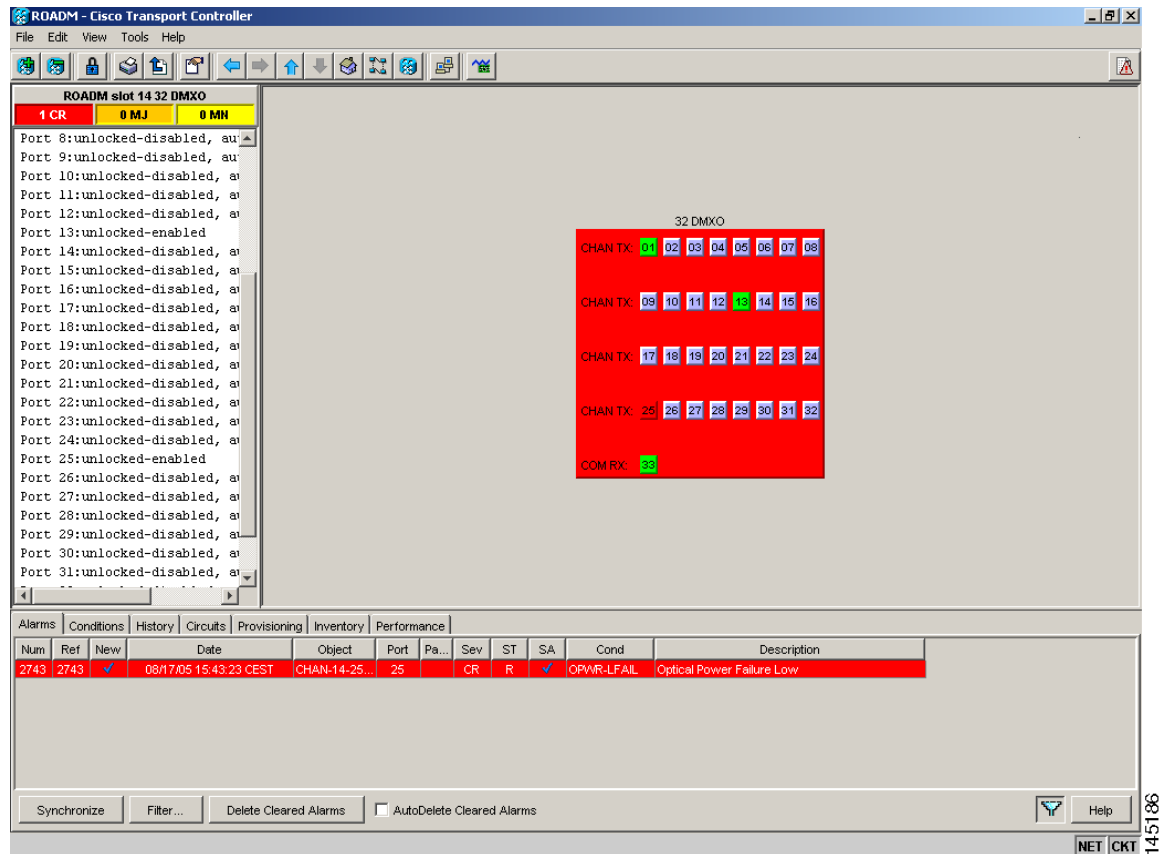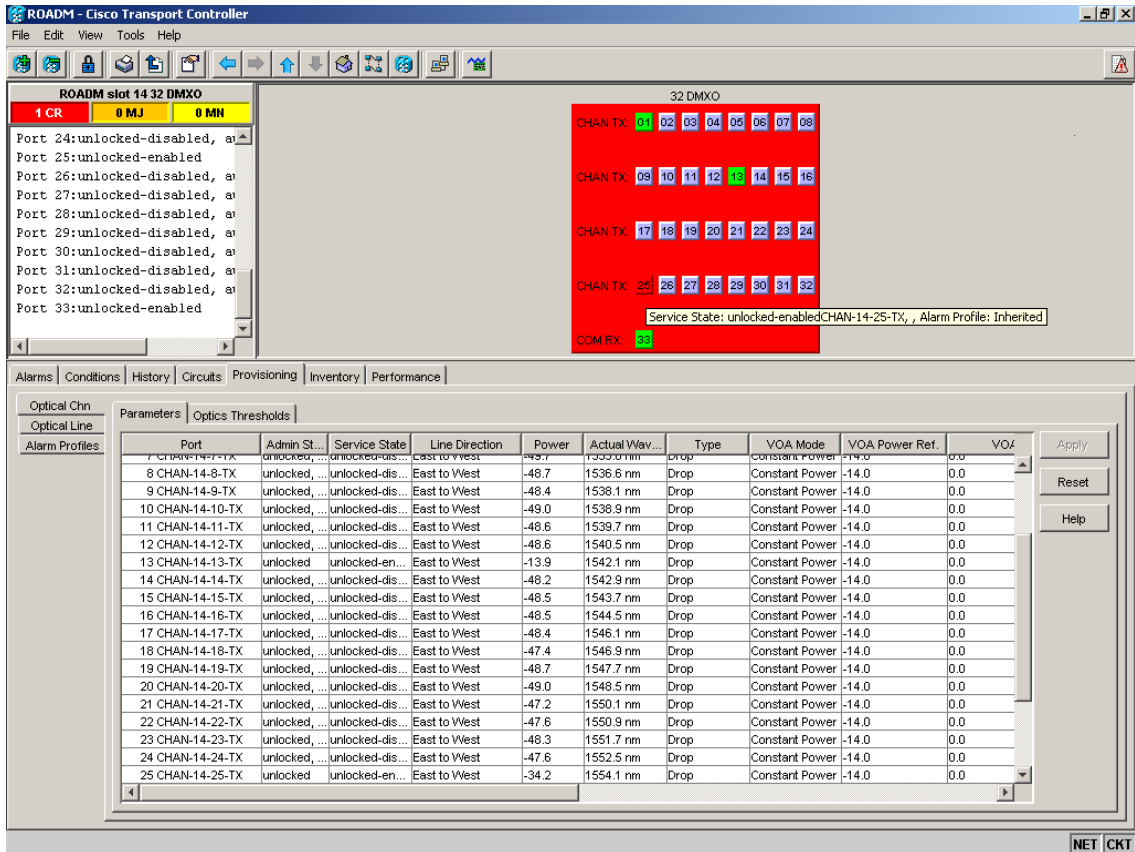

1.13.2.3.2 Condition C2—Delta Power < 6 dB Lower than Expected

If the delta power is less than 6 dB lower than expected, the final conditions reported in CTC are the same as those reported for ConditionB2 (see 1.13.2.2.2 Condition B2—Delta Power < 6 dB (OPWR-LowDEGrade Alarm), page 1-87):

- An OPWR-LowDEGrade (OCH layer) alarm is present on the port associated with the VOA.

- A valid (different from the end of scale value of – 50dBm) optical power value can be read in the CTC Power field, but the value is (VOA Power Ref – 6 dBm) < Power < VOA Power Ref (Figure 1-34). To view this value in card view, click the **Provisioning > Parameters** tabs.).

A dirty connection or excessive loss of the incoming span are among the possible reasons that can lead to a fault condition. They are the most common and affect all wavelengths, whereas an excessive amplifier gain tilt or a wavelength misconfiguration on the far-end TXP or MXP card can lead to condition where only a single wavelength fails, such as the one (Channel 25) shown in Figure 1-36.

Figure 1-36   ***Optical Drop Power Less than 6 dB Lower than Expected***

1.13.2.3.3 Corrective Action for Scenario C (Optical Power Level of Incoming Signal Lower than Expected)

If condition C1 (see "1.13.2.3.1 Condition C1—Delta Power > 6 dB Lower than Expected" section on page 1-94) results in an LOS-P alarm, compete the following procedure:

Step 1 Verify the alarm validity:

a. Identify the DWDM nodes where the alarmed card is located.

b. Double-click the 32DMX-O card.

c. Click **Alarms**.

d. Verify that a LOS-P alarm is present on the CHAN-TX port.

e. Click the **Synchronize** button at the bottom left of the window.

f. If the alarm is correctly reported, move to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again.

Note If the alarm inconsistency persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 2 Verify the correct behavior of the far-end DWDM card (32MUX-O, 32WSS, AD-xC-xx.x) that manages the channel (wavelength), and the TXP, MXP, or line card that is the signal source of the channel (wavelength) alarmed:

a. Click **Circuits** and retrieve the node, card, and port information for the alarmed channel from the Source field of the OCHNC circuit.

b. For the far-end DWDM card, verify that the power value coming in the ADD_RX port is correct:

  • In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

✎ **Note** *X* is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

  • The Power field value must be the same of VOA Power Ref field. If not, take the appropriate corrective actions according to Chapter 2, "Alarm Troubleshooting."

c. For the corresponding TXP, MXP, or line card connected, verify the following:

  • The TX laser is active (the trunk port is in IS [unlocked] state).

  • The wavelength provisioned is the proper one.

d. The output power value must be within the expected range (refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC (for example, TXP_MR_2.5G), perform a manual measurement using a standard power meter.

e. If everything in Step 2 is correct, go to Step 3. If not, take the appropriate corrective actions according to Chapter 2, "Alarm Troubleshooting."

Step 3 Verify the correct behavior of the VOA inside the 32DMX-O card:

a. Double-click the 32DMX-O card.

b. Click **Circuits**.

c. Delete the OCHNC circuit for the faulty channel.

d. Ensure that the service state of the corresponding CHAN-TX port changes to IS-AINS (or unlocked, automaticInService) and the color changes to grey (LOS-P alarm should clear).

e. Click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs and identify the proper channel (wavelength).

✎ **Note** *X* is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

f. Decrease the attenuation on the VOA to the minimum (0 dB) to enable channel startup. To perform this in field adjustment:

  • Read the **VOA Attenuation Ref** value for the channel (wavelength).

  • Enter the same value into the VOA Attenuation Calib field as that in the VOA Attenuation Ref field, but with the opposite sign (the algebraic sum of the two contributions must be equal to zero).

  • Click **Apply**.

g. Click **Circuits**.

h. Recreate the OCHNC circuit and verify that Circuit Status field reports DISCOVERED and the state is IS (unlocked).

i. If the LOS-P alarm has not cleared, continue with . If it has cleared, you are finished.

Step 4 To unambiguously pinpoint the root cause of the alarm, verify the proper cabling of the COM-RX port (common input port for all the drop channels) of the alarmed 32DMX-O card:

a. Verify that the COM_RX port of the alarmed 32DMX-O is connected either to the DROP_TX port of a 32WSS card or to the COM_TX port of an OPT-PRE, OPT-BST, or OSC-CSM card, depending on the actual node layout.

b. Pull out the LC connector from the COM_RX port of the 32DMX-O card and clean the fiber according to site practice.

c. Pull out the LC connector from the COM_TX or DROP_TX port of the connected DWDM card and clean the fiber according to site practice.

d. Verify that the fiber attenuation is within the specifications (maximum tolerance is 1 dB).

e. If necessary, replace any bad fibers.

> ✎
> **Note**   If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

f. If the alarm condition persists even after the cabling has been checked and fixed, replace the 32DMX-O card (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Before replacing the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem).

If condition C2 (see) results in an OPWR-LowDEGrade alarm, compete the following procedure:

Step 1 Verify the alarm validity:

a. Identify the DWDM nodes where the alarmed card is seated.

b. Double-click the 32DMX-O card.

c. Click **Alarms**.

d. Verify that an Optical Power Degrade Low Loss of incoming Payload (OPWR-LDEG) alarm is present on the CHAN-TX port.

e. Click the **Synchronize** button at the bottom left of the window.

f. If the alarm is correctly reported, move to . If not, close the CTC application, delete the CTC cache, and open the CTC connection again.

> ✎
> **Note**   If the alarm inconsistency persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 2   Verify the correct behavior of the far-end DWDM card (32MUX-O, 32WSS, or AD-xC-xx.x) that manages the channel (wavelength) and the TXP, MXP, or line card that is the signal source of the channel (wavelength) alarmed.

    a. Click **Circuits** and retrieve the node, card, and port information for to the alarmed channel from the Source field of the OCHNC circuit.

    b. For the far-end DWDM card, verify that the power value coming in on the ADD_RX port is correct:

       • In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

> **Note**   *X* is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

       • The Power field value must be the same of VOA Power Ref field. If not, take the appropriate corrective actions according to Chapter 2, "Alarm Troubleshooting."

    c. For the corresponding TXP, MXP, or line card connected, verify the following:

       • The TX laser is active (the trunk port is in IS [unlocked] state).

       • The wavelength provisioned is the proper one.

    d. The output power value must be within the expected range (refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

    e. If everything in Step 2 is correct, move to Step 3. If not, take the appropriate corrective actions according to Chapter 2, "Alarm Troubleshooting."

Step 3   Verify the proper cabling of the COM-RX port (the common input port for all of the drop channels) of the alarmed 32DMX-O:

    a. Verify that the COM_RX port of the alarmed 32DMX-O is connected either to the DROP_TX port of a 32WSS card or to the COM_TX port of an OPT-PRE, OPT-BST, or OSC-CSM, depending on the actual node layout.

    b. Pull out the LC connector from the COM_RX port of the 32DMX-O card and clean the fiber according to site practice.

    c. Pull out the LC connector from the COM_TX or DROP_TX port of the connected DWDM card and clean the fiber according to site practice.

    d. Verify that the fiber attenuation is within the specifications (maximum tolerance is 1 dB).

    e. If necessary, replace any bad fibers.

> **Note**   If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

    f. If the alarm condition persists even after the cabling has been checked and fixed, the root cause could be related to a network issue and a more accurate analysis of the signal flow is needed according to the actual system topology. If necessary, call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.