General Troubleshooting

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

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

This chapter includes the following sections on network problems:

- Network Troubleshooting Tests—Describes loopbacks and hairpin circuits, which you can use to test circuit paths through the network or logically isolate faults.

  Note For network acceptance tests, refer to the *Cisco ONS 15454 Procedure Guide*.

- Identify Points of Failure on a DS-N Circuit Path—Explains how to perform the tests described in the "1.1 Network Troubleshooting Tests" section on a DS-N circuit.
- Using the DS3XM-6 Card FEAC (Loopback) Functions—Describes the far-end alarm and control (FEAC) functions on the DS3XM-6 card.
- Identify Points of Failure on an Optical Circuit Path—Explains how to perform the tests described in the "1.1 Network Troubleshooting Tests" section on an OC-N circuit.

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

- Restoring the Database and Default Settings—Provides procedures for restoring software data and restoring the node to the default setup.
- PC Connectivity Troubleshooting—Provides troubleshooting procedures for PC and network connectivity to the ONS 15454.
- CTC Operation Troubleshooting—Provides troubleshooting procedures for CTC login or operation problems.
- Circuits and Timing—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.

- Fiber and Cabling—Provides troubleshooting procedures for fiber and cabling connectivity errors.
- Power and LED Tests—Provides troubleshooting procedures for power supply and LED indicator problems.

1.1 Network Troubleshooting Tests

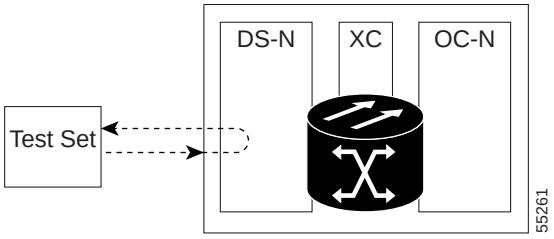
Use loopbacks and hairpin circuits to test newly created SONET circuits before running live traffic or to logically locate the source of a network failure. All ONS 15454 OC-N cards, transponder cards (TXP, TXPP), muxponder (MXP) cards, and G-Series Ethernet cards allow loopbacks and hairpin test circuits. Other cards do not allow loopbacks. These include ONS E-Series Ethernet, ML-Series Ethernet, and DWDM cards such as OPT-BST, OPT-PRE, OSC-CSM, band add-drop cards, and channel add-drop cards.

Caution Facility (line) or terminal loopbacks can be service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. For more information about these operations, refer to the *Cisco ONS 15454 Procedure Guide*.

Caution On OC-N cards, a facility (line) loopback applies to the entire card and not an individual circuit. Exercise caution when using loopbacks on an OC-N card carrying live traffic.

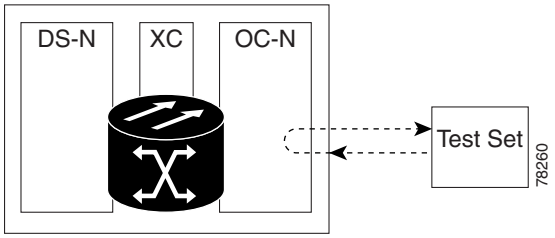
A facility (line) loopback tests the line interface unit (LIU) of a card, the EIA (electrical interface assembly), and related cabling. After applying a facility loopback on a port, use a test set to run traffic over the loopback. A successful facility loopback isolates the LIU, the EIA, or the cabling plant as the potential cause of a network problem. Figure 1-1 shows a facility loopback on a DS-N card.

Figure 1-1 Facility (Line) Loopback Process on a DS-N Card



To test the LIU on an OC-N card, connect an optical test set to the OC-N port and perform a facility (line) loopback or use a loopback or hairpin circuit on a card that is farther along the circuit path. Figure 1-2 shows a facility loopback on an OC-N card.

Figure 1-2 Facility (Line) Loopback Process on an OC-N Card



Caution Before performing a facility (line) loopback on an OC-N card, be sure 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 ONS 15454 containing the loopback OC-N card.

A terminal loopback tests a circuit path as it passes through the cross-connect card (XC10G) and loops back from the card with the loopback. Figure 1-3 shows a terminal loopback on an OC-N card. (Ethernet, transponder, and muxponder loopbacks follow the same model.) The test-set traffic comes into the DS-N card and goes through the cross-connect card to the OC-N card. The terminal loopback on the OC-N card turns the signal around before it reaches the LIU and sends it back through the cross-connect card to the DS-N card. This test verifies that the cross-connect card and terminal circuit paths are valid, but does not test the LIU on the OC-N card.

Setting a terminal loopback on the G-Series card might not stop the Tx Packets counter or the Rx Packet counters on the CTC card-level view Performance > Statistics page from increasing. The counters can increment even though the loopbacked port has temporarily disabled the transmit laser and is dropping any received packets.

The Tx Packet statistic continues to increment because the statistic is not based on the packets transmitted by the transmit (Tx) laser but on the Tx signal inside the G-Series card. In normal in-service port operation, the Tx signal being recorded does result in the Tx laser transmitting packets, but in a terminal loopback this signal is being looped back within the G-Series card and does not result in the Tx laser transmitting packets.

The Rx Packet counter might also continue to increment when the G-Series card is in terminal loopback. Receive (Rx) packets from any connected device are dropped and not recorded, but the internally looped back packets follow the G-Series card's normal receive path and register on the Rx Packet counter.

Figure 1-3 Terminal Loopback Process on an OC-N Card

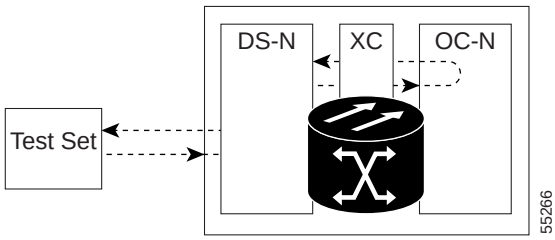
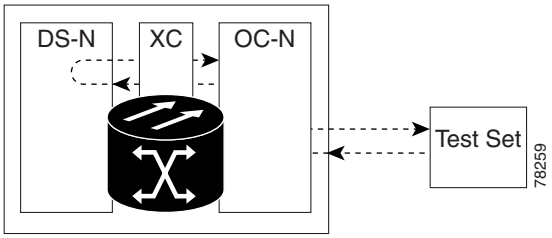


Figure 1-4 shows a terminal loopback on a DS-N card. The test-set traffic comes in on the OC-N card and goes through the cross-connect card to the DS-N card. The terminal loopback on the DS-N card turns the signal around before it reaches the LIU and sends it back through the cross-connect card to the OC-N card. This test verifies that the cross-connect card and terminal circuit paths are valid, but does not test the LIU on the DS-N card.

Figure 1-4 Terminal Loopback Process on a DS-N Card



ONS 15454 port loopbacks either terminate or bridge the loopback signal. In the ONS 15454 system, all optical, electrical, Ethernet, and TXP/MXP facility loopbacks are terminated as shown in Table 1-1. During terminal loopbacks, some ONS cards bridge the loopback signal while others terminate it.

If an optical, electrical, Ethernet, and TXP/MXP port terminates a terminal or facility loopback signal, this means that 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.

All ONS 15454 card bridging and terminating behaviors are listed in Table 1-1. When a port on a card in the left column of this table originates a terminal or facility loopback, the signal behaves as listed in the middle and right columns.

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

Table 1-1 DS-N, OC-N, EC-N, and TXP/MXP Card Loopback Behavior

Card/Port	Terminal loopback signal	Facility loopback signal
DS-1	Terminated	Terminated
DS-3	Bridged	Terminated
DS-N transmux	Bridged	Terminated
All OC-N cards	Bridged	Terminated
EC-1	Bridged	Terminated
G-Series Ethernet	Terminated[1]	Terminated[2]
TXP_MR_2.5G	Bridged	Terminated
TXP_MR_10G	Bridged	Terminated[3]
MXP_2.5G_10G	Bridged	Terminated[4]

1. G-Series Ethernet terminal loopback is terminated and Ethernet transmission is disabled. No AIS is inserted for Ethernet, but a TPTFAIL alarm is raised on the far-end Ethernet port.
2. G-Series facility loopback is terminated and no AIS is sent downstream. However, the Cisco Link Integrity signal continues to be sent downstream.

3. A facility loopback on the client or trunk squelches the far end.
4. A facility loopback when the card is in transparent mode on the client or trunk squelches the far end.

The loopback itself is listed in the Alarms window. For example, the window would list the LPBKTERMINAL condition or LPBKFACILITY condition for a tested port.

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

- If a DS-N, OC-N, or EC-1 port is placed in out of service (OOS) state, it injects an AIS signal upstream and downstream.
- If a DS-N, OC-N, or EC-1 port is placed in out of service auto in-service (OOS_AINS) state or in the out of service maintenance (OOS_MT) state before loopback testing, the port clears the AIS signal upstream and downstream unless there is a service-affecting defect that would also cause an AIS signal to be injected. For more information about placing ports into alternate states for testing, refer to the *Cisco ONS 15454 Procedure Guide*.
- If a TXP_MR_2.5G port is placed in the out of service maintenance (OOS_MT) state before loopback testing, the port raises an Alarms Suppressed for Maintenance (AS-MT) condition during the loopback on the client side port.
- If a TXP_MR_10G port is placed in the out of service maintenance (OOS_MT) state before loopback testing, the port raises a Loss of Signal (LOS) alarm on the DWDM-side port during the loopback.
- If an MXP_2.5_10G port is placed in the out of service maintenance (OOS_MT) state before loopback testing, the port raises a Loss of Signal (LOS) alarm on the DWDM-side port during the loopback.

Bridged DS-N and OC-N terminal loopback examples are shown in Figure 1-5 and Figure 1-6.

Figure 1-5 Terminal Loopback on a DS-N Card with Bridged Signal

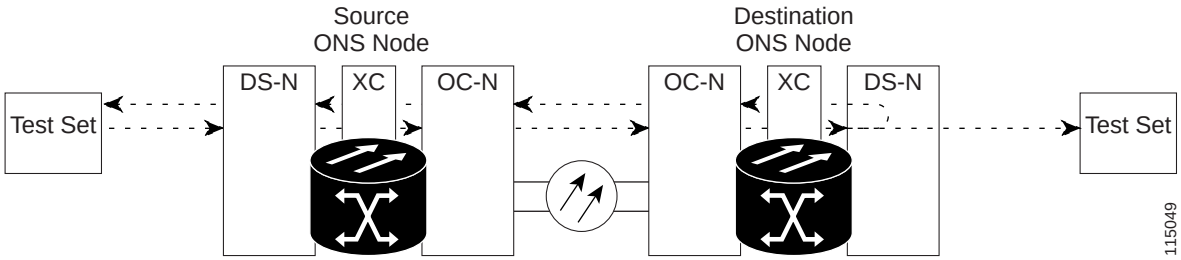
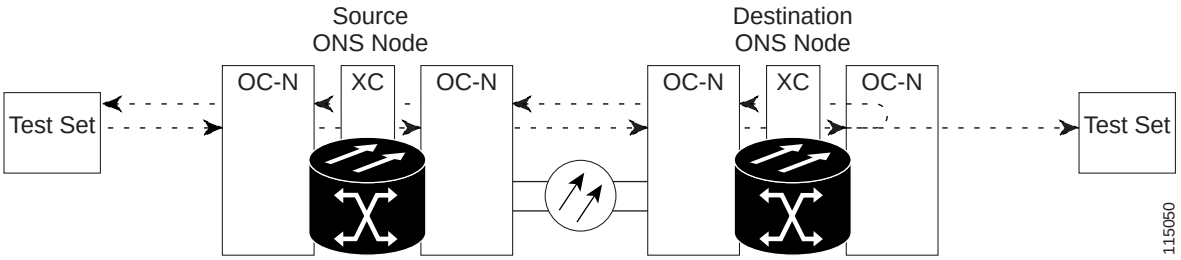
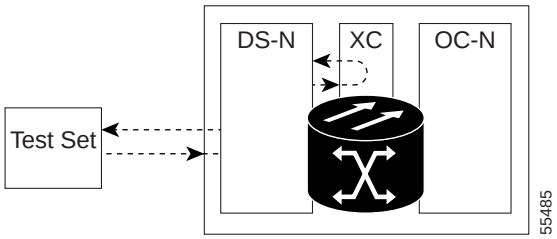


Figure 1-6 Terminal Loopback on an OC-N Card with Bridged Signal



A hairpin circuit brings traffic in and out on a DS-N port rather than sending the traffic onto the OC-N card. A hairpin loops back only the specific STS or VT circuit and does not cause an entire OC-N port to loop back, thus preventing a drop of all traffic on the OC-N port. The hairpin allows you to test a specific STS or VT circuit on nodes running live traffic. Figure 1-9 shows the hairpin circuit process on a DS-N card.

Figure 1-7 Hairpin Circuit Process on a DS-N Card



A cross-connect loopback tests a circuit path as it passes through the cross-connect card and loops back to the port being tested. Testing and verifying circuit integrity often involves taking down the whole line; however, a cross-connect loopback allows you to create a loopback on any embedded channel at supported payloads at the STS-1 granularity and higher. For example, you can loop back a single STS-1, STS-3c, STS-6c, etc. on an optical facility (line) without interrupting the other STS circuits.

The following restrictions apply to cross-connect loopbacks:

- You can create a cross-connect loopback on all working or protect optical ports unless the protect port is used in a 1+1 protection group and is in working mode.
- If a terminal or facility loopback exists on a port, you cannot use the cross-connect loopback.

1.2 Identify Points of Failure on a DS-N Circuit Path

Facility (line) loopbacks, terminal (inward) loopbacks, and hairpin circuits are often used to test a 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.

The example in this section tests a DS-N circuit on a two-node, bidirectional line switched ring (BLSR). Using a series of facility loopbacks, terminal loopbacks, and hairpins, the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of five network test procedures apply to this sample scenario:

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

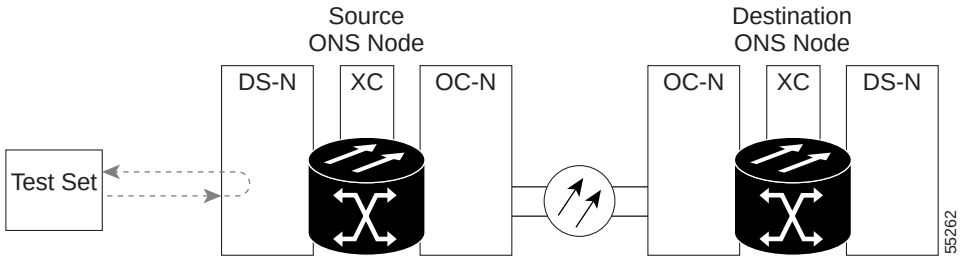
1. A facility (line) loopback on the source node DS-N
2. A hairpin on the source node DS-N
3. A terminal (inward) loopback on the destination node DS-N
4. A hairpin on the destination node DS-N
5. A facility (line) loopback on the destination DS-N

Note All loopback tests require on-site personnel.

1.2.1 Perform a Facility (Line) Loopback on a Source DS-N Port

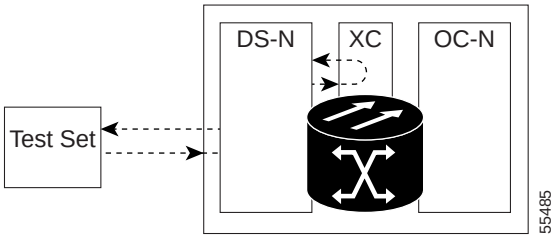
The facility (line) loopback test is performed on the node source port in the network circuit, in this example, the DS-N port in the source node. Completing a successful facility (line) loopback on this port isolates the cabling, the DS-N card, and the EIA as possible failure points. Figure 1-10 shows an example of a facility loopback on a source DS-N port.

Figure 1-8 A Facility (Line) Loopback on a Circuit Source DS-N Port



A hairpin circuit brings traffic in and out on a DS-N port rather than sending the traffic onto the OC-N card. A hairpin loops back only the specific STS or VT circuit and does not cause an entire OC-N port to loop back, thus preventing a drop of all traffic on the OC-N port. The hairpin allows you to test a specific STS or VT circuit on nodes running live traffic. Figure 1-9 shows the hairpin circuit process on a DS-N card.

Figure 1-9 Hairpin Circuit Process on a DS-N Card



A cross-connect loopback tests a circuit path as it passes through the cross-connect card and loops back to the port being tested. Testing and verifying circuit integrity often involves taking down the whole line; however, a cross-connect loopback allows you to create a loopback on any embedded channel at supported payloads at the STS-1 granularity and higher. For example, you can loop back a single STS-1, STS-3c, STS-6c, etc. on an optical facility (line) without interrupting the other STS circuits.

The following restrictions apply to cross-connect loopbacks:

- You can create a cross-connect loopback on all working or protect optical ports unless the protect port is used in a 1+1 protection group and is in working mode.
- If a terminal or facility loopback exists on a port, you cannot use the cross-connect loopback.

1.3 Identify Points of Failure on a DS-N Circuit Path

Facility (line) loopbacks, terminal (inward) loopbacks, and hairpin circuits are often used to test a 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.

The example in this section tests a DS-N circuit on a two-node, bidirectional line switched ring (BLSR). Using a series of facility loopbacks, terminal loopbacks, and hairpins, the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of five network test procedures apply to this sample scenario:

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

West to east direction (left to right):

1. A facility (line) loopback on the source node DS-N
2. A hairpin on the source node DS-N
3. An XC loopback on the destination node OC-N STS (carrying the DS-N circuit)
4. A terminal (inward) loopback on the destination node DS-N

East to west direction (right to left):

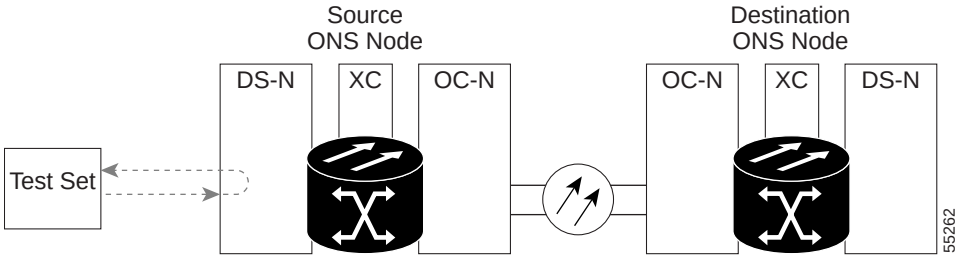
1. A facility (line) loopback on the destination node DS-N
2. A hairpin on the destination node DS-N
3. An XC loopback on the source node OC-N STS (carrying the DS-N circuit)
4. A terminal (inward) loopback on the source node DS-N

Note All loopback tests require on-site personnel.

1.3.1 Perform a Facility (Line) Loopback on a Source DS-N Port (West to East)

The facility (line) loopback test is performed on the node source port in the network circuit, in this example, the DS-N port in the source node. Completing a successful facility (line) loopback on this port isolates the cabling, the DS-N card, and the EIA as possible failure points. Figure 1-10 shows an example of a facility loopback on a source DS-N port.

Figure 1-10 A Facility (Line) Loopback on a Circuit Source DS-N Port



Caution Performing a loopback on an in-service circuit is service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. For more information about these operations, refer to the *Cisco ONS 15454 Procedure Guide*.

Note DS-3 facility (line) loopbacks do not transmit an alarm indication signal (AIS) condition in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

Create the Facility (Line) Loopback on the Source DS-N Port

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

Use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the EIA connectors or DSx panel for the port you are testing. The Tx and Rx terminals connect to the same port. Adjust the test set accordingly.

Step 2 In node view, double-click the DS-N card to open the card view.

Step 3 Depending upon the card type, click the **Maintenance** > **Loopback** tabs, **Maintenance** > **DS1** tabs, or **Maintenance** > **DS3** tabs.

Step 4 Choose **OOS_MT** from the State column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested.

Step 5 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 port being tested.

Step 6 Click **Apply**.

Step 7 Click **Yes** in the confirmation dialog box.

Note It is normal for the "LPBKFACILITY (DS1, DS3)" condition on page 2-141 to appear during loopback setup. The condition clears when you remove the loopback.

Step 8 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-9.

Test and Clear the Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Double-click the card to open the card view.

Step 4 Depending upon the card type, click the **Maintenance** > **Loopback** tabs, **Maintenance** > **DS1** tabs, or **Maintenance** > **DS3** tabs.

Step 5 Choose **None** from the Loopback Type column for the port being tested.

Step 6 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty DS-N card, faulty cabling from the DS-N card to the DSx panel or the EIA, or a faulty EIA.

Step 10 Complete the "Test the DS-N Cabling" procedure on page 1-10.

Test the DS-N Cabling

Step 1 Replace the suspected bad cabling (the cables from the test set to the DSx panel or the EIA ports) with a known-good cable.

If a known-good cable is not available, test the suspected bad cable with a test set. Remove the suspected bad cable from the DSx panel or the EIA and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or defective.

Step 2 Resend test traffic on the loopback circuit with a known-good cable installed. If the test set indicates a good circuit, the problem was probably the defective cable.

Step 3 Replace the defective cable.

Step 4 In card view for the DS-N card, depending upon the type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

Step 5 Choose **None** from the Loopback Type column for the port being tested.

Step 6 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty card or a faulty EIA.

Step 10 Complete the "Test the DS-N Card" procedure on page 1-10.

Test the DS-N Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the Return Materials Authorization (RMA) process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the faulty card.

Step 5 In card view for the DS-N card, depending upon the type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

Step 6 Choose **None** from the Loopback Type column for the port being tested.

Step 7 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 8 Click **Apply**.

Step 9 Click **Yes** in the confirmation dialog box.

Step 10 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty EIA.

Step 11 Complete the "Test the EIA" procedure on page 1-11.

Test the EIA

Note This procedure does not apply to Software R4.6 DWDM cards or ML-Series cards.

Step 1 Remove and reinstall the EIA to ensure a proper seating:

- **a.** Remove the lower backplane cover. Loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.
- **b.** Loosen the nine perimeter screws that hold the EIA panel in place.
- **c.** Lift the EIA panel by the bottom to remove it from the shelf assembly.
- **d.** Follow the installation procedure for the appropriate EIA. See the "Replace an Electrical Interface Assembly" procedure on page 3-17.

Step 2 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the reinstalled EIA. If the test set indicates a good circuit, the problem was probably an improperly seated EIA, and you can proceed to Step 16. If the problem persists and the EIA is not shown to be improperly seated, proceed to Step 3.

Step 3 In card view for the DS-N card, depending upon the type, click the **Maintenance** > **Loopback** tabs, **Maintenance** > **DS1** tabs, or **Maintenance** > **DS3** tabs.

Step 4 Choose **None** from the Loopback Type column for the port being tested.

Step 5 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 6 Click **Apply**.

Step 7 Click **Yes** in the confirmation dialog box. Proceed to Step 16.

Step 8 If the test set indicates a faulty circuit, the problem is probably a defective EIA. Return the defective EIA to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 9 Replace the faulty EIA. See the "Replace an Electrical Interface Assembly" procedure on page 3-17.

Step 10 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement EIA. If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

Step 11 If the test set indicates a good circuit, the problem was probably the defective EIA. Clear the facility (line) loopback by clicking the **Maintenance** > **Loopback** tabs, **Maintenance** > **DS1** tabs, or **Maintenance** > **DS3** tabs.

Step 12 Choose **None** from the Loopback Type column for the port being tested.

Step 13 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 14 Click **Apply**.

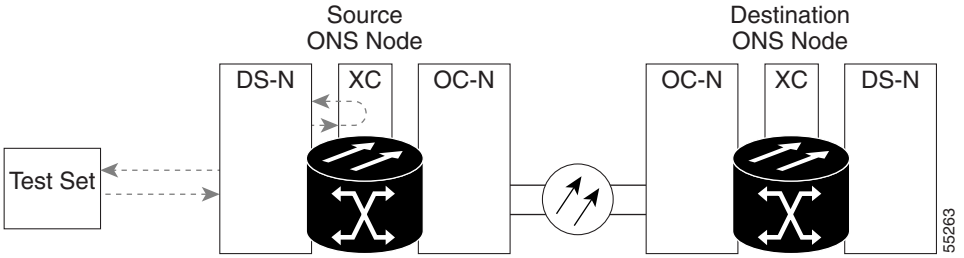
Step 15 Click **Yes** in the confirmation dialog box.

Step 16 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12.

1.3.2 Perform a Hairpin Test on a Source Node Port (West to East)

The hairpin test is performed on the cross-connect card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through the port isolates the possibility that the cross-connect card is the cause of the faulty circuit. Figure 1-11 shows an example of a hairpin loopback on a source node port.

Figure 1-11 Hairpin on a Source Node Port



Note The ONS 15454 does not support simplex operation on the XC10G cross-connect card. Two cross-connect cards of the same type must be installed for each node.

Create the Hairpin Circuit on the Source Node Port

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

- **a.** If you just completed the "Perform a Facility (Line) Loopback on a Source DS-N Port (West to East)" procedure on page 1-8, leave the electrical test set hooked up to the DS-N port in the source node.
- **b.** If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. The Tx and Rx terminals connect to the same port.
- **c.** Adjust the test set accordingly.

Step 2 Use CTC to set up the hairpin circuit on the test port:

- **a.** In node view, click the **Circuits** tab and click **Create**.
- **b.** In the Circuit Creation dialog box, choose the type and size, such as an STS-1.
- **c.** Click **Next**.
- **d.** In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "Hairpin1."
- **e.** Uncheck the **Bidirectional** check box.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) used for the source dialog box.

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab and that the **Dir** column describes it as a one-way circuit.

Step 4 Complete the "Test and Delete the Hairpin Circuit" procedure on page 1-13.

Test and Delete the Hairpin 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 received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the hairpin circuit. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits box.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

Step 4 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18. If the test set indicates a faulty circuit, there might be a problem with the XC10G card.

Step 5 Complete the "Test the Standby XC10G Cross-Connect Card" procedure on page 1-13.

Test the Standby XC10G Cross-Connect Card

Note Two XC10G cross-connect cards (active and standby) must be in use on a node to use this procedure.

Step 1 Perform a reset on the standby XC10G cross-connect card to make it the active card:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

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

Step 2 Initiate an external switching command (side switch) on the cross-connect cards before you retest the loopback circuit:

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby XC10G cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. In the node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active XC10G cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 4 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

Step 5 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 6 To confirm a defective original cross-connect card, complete the "Retest the Original XC10G Cross-Connect Card" procedure on page 1-14.

Retest the Original XC10G Cross-Connect Card

Step 1 Initiate an external switching command (side switch) on the XC10G cross-connect cards:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. In node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. From the Cross-Connect Cards menu, choose **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447) and proceed to Step 4. If the test does not indicate a faulty circuit, proceed to Step 5.

Step 4 Complete the "Replace an In-Service Cross-Connect Card" procedure on page 3-2 for the defective cross-connect card.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

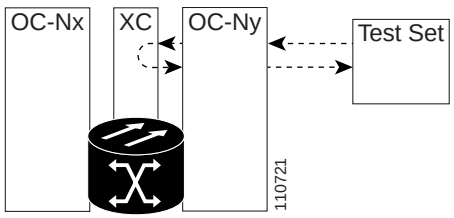
Step 6 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18.

1.3.3 Perform an XC Loopback on a Destination Node OC-N STS (West to East)

The XC loopback tests whether any problem exists on the circuit's OC-N span, isolating this span from others present on the card. The loopback occurs on the XC10G cross-connect card in a network circuit. Figure 1-12 shows an example of an XC loopback on a destination OC-N port.

Note The XC Loopback on an OC-N card does not affect traffic on other circuits.

Figure 1-12 XC Loopback on a Destination OC-N Port



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

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

a. If you just completed the "1.5.2 Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" section on page 1-40, leave the optical test set hooked up to the destination node port.

b. If you are starting the current procedure without the optical test set hooked up to the destination port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. The Tx and Rx terminals connect to the same port.

c. Adjust the test set accordingly.

Step 2 Use CTC to put the circuit being tested out of service:

a. In node view, click the **Circuits** tab.

b. Click the circuit and then click **Edit**.

c. In the Edit Circuit dialog box, click the State tab.

d. Choose **OOS-MT** from the Target Circuit State drop-down list.

e. Click **Apply**.

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

Step 3 Use CTC to set up the XC loopback on the circuit being tested:

a. In node view, double-click the OC-N card to open the card view.

b. Click the **Provisioning > SONET STS** tabs.

c. Click the check box in the XC Loopback column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog.

Step 4 Complete the "Test the XC Loopback Circuit" procedure on page 1-45.

Test the XC Loopback Circuit

Note This procedure is performed only on OC-N cards.

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the cross-connect. Clear the XC loopback:

a. In card view, click the **Provisioning > SONET STS** tabs.

b. Uncheck the check box in the XC Loopback column for the circuit being tested.

c. Click **Apply**.

d. Click **Yes** in the confirmation dialog.

Step 4 Complete the "Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-48. If the test set indicates a faulty circuit, there might be a problem with the cross-connect card.

Step 5 Complete the "Test the Standby XC10G Cross-Connect Card" procedure on page 1-45.

Test the Standby XC10G Cross-Connect Card

Step 1 Perform a reset on the standby cross-connect card:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

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

Step 2 Initiate an external switching command (side switch) on the cross-connect cards before you retest the loopback circuit:

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. In the node view, select the **Maintenance** > **Cross-Connect** > **Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 4 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

e. Confirm that the XC loopback circuit is deleted form the Circuits tab list. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC10G Cross-Connect Card" procedure on page 1-46.

Retest the Original XC10G Cross-Connect Card

Note This procedure is performed only on OC-N and XC10G cards.

Step 1 Initiate an external switching command (side switch) on the cross-connect cards.

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. In node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447) and proceed to Step 4. If the circuit is not shown to be faulty and the card is not shown to be defective, you are finished with testing.

Step 4 Complete the "Replace an In-Service Cross-Connect Card" procedure on page 3-2 for the defective cross-connect card and perform Step 5.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

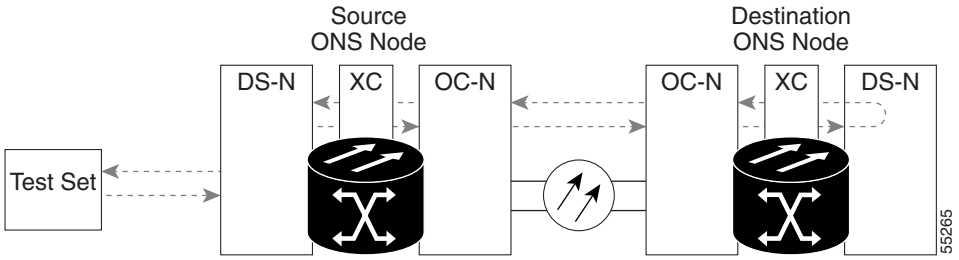
d. Click **Yes** in the Delete Circuits dialog box.

1.3.4 Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)

The terminal (inward) loopback test is performed on the node destination port in the circuit, such as a destination node DS-N port. You create a bidirectional circuit that starts on the source node DS-N port and loops back on the destination node DS-N port. Then you proceed with the terminal loopback test.

Completing a successful terminal loopback to a destination node DS-N port verifies that the circuit is good to the destination DS-N. Figure 1-13 shows an example of a terminal loopback on a destination DS-N port.

Figure 1-13 Terminal (Inward) Loopback on a Destination DS-N Port



Caution Performing a loopback on an in-service circuit is service-affecting. To protect traffic, apply a lockout or force switch to the target loopback port. For more information about these operations, refer to the *Cisco ONS 15454 Procedure Guide*.

Note DS-3 terminal loopbacks do not transmit an AIS condition in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

Create the Terminal (Inward) Loopback on a Destination DS-N Port

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

- **a.** If you just completed the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12, leave the electrical test set hooked up to the DS-N port in the source node.
- **b.** If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. Both Tx and Rx connect to the same port.
- **c.** Adjust the test set accordingly.

Step 2 In CTC node view, click the **Circuits** tab and click **Create**.

Step 3 In the Circuit Creation dialog box, choose the type and size, such as an STS-1.

Step 4 Click **Next**.

Step 5 In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "DS-NtoDS-N."

Step 6 Leave the **Bidirectional** check box checked.

Step 7 Click **Next**.

Step 8 In the Circuit Creation source dialog box, select the **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.

Step 9 Click **Next**.

Step 10 In the Circuit Creation destination dialog box, use the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) used for the source dialog box.

Step 11 Click **Finish**.

Step 12 Confirm that the newly created circuit appears in the **Dir** column as a 2-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)" condition on page 2-144 to appear during a loopback setup. The condition clears when you remove the loopback.

Note DS-3 terminal loopbacks do not transmit a DS-3 AIS (see the "AIS" condition on page 2-21) in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

Step 13 Create the terminal (inward) 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, such as the DS-N card in the destination node.

c. Depending upon the card type, click the **Maintenance** > **Loopback** tabs, **Maintenance** > **DS1** tabs, or **Maintenance** > **DS3** tabs.

d. Select **OOS_MT** from the 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 14 Complete the "Test and Clear the Terminal (Inward) Loopback Circuit on the Destination DS-N Port" procedure on page 1-20.

Test and Clear the Terminal (Inward) Loopback Circuit on the Destination DS-N Port

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Double-click the DS-N card in the destination node with the terminal loopback.

Step 4 Depending upon the card type, click the **Maintenance** > **Loopback** tabs, **Maintenance** > **DS1** tabs, or **Maintenance** > **DS3** tabs.

Step 5 Select **None** from the Loopback Type column for the port being tested.

Step 6 Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Clear the terminal loopback:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 10 Complete the "Perform a Hairpin Test on a Destination Node Port (East to West)" procedure on page 1-25. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 11 Complete the "Test the Destination DS-N Card" procedure on page 1-21.

Test the Destination DS-N Card

Note This procedure does not apply to Software R4.6 DWDM cards or ML-Series cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the defective DS-N card.

Step 5 Clear the terminal (inward) loopback state on the port:

a. Double-click the DS-N card in the destination node with the terminal loopback.

b. Depending upon the card type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

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

d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 6 Delete the terminal (inward) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

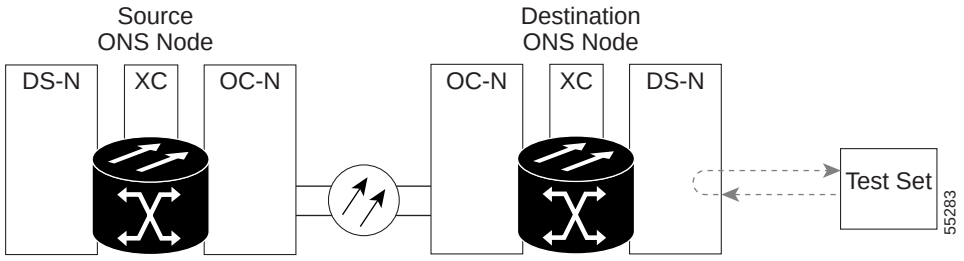
d. Click **Yes** in the Delete Circuits dialog box.

Step 7 Complete the "Perform a Hairpin Test on a Destination Node Port (East to West)" procedure on page 1-25.

1.3.5 Perform a Facility (Line) Loopback on a Destination DS-N Port (East to West)

The facility (line) loopback test is performed on the node destination port in the network circuit, in this example, the DS-N port in the destination node. Completing a successful facility (line) loopback on this port isolates the cabling, the DS-N card, and the EIA as possible failure points. Figure 1-14 shows an example of a facility loopback on a destination DS-N port.

Figure 1-14 A Facility (Line) Loopback on a Circuit Destination DS-N Port



Caution Performing a loopback on an in-service circuit is service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. For more information about these operations, refer to the *Cisco ONS 15454 Procedure Guide*.

Note DS-3 facility (line) loopbacks do not transmit an alarm indication signal (AIS) condition in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

Create the Facility (Line) Loopback on the Destination DS-N Port

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

Use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the EIA connectors or DSx panel for the port you are testing. The Tx and Rx terminals connect to the same port. Adjust the test set accordingly.

Step 2 In CTC node view, double-click the DS-N card to open the card view.

Step 3 Depending upon the card type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

Step 4 Choose **OOS_MT** from the State column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested.

Step 5 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 port being tested.

Step 6 Click **Apply**.

Step 7 Click **Yes** in the confirmation dialog box.

Note It is normal for a "LPBKFACILITY (DS1, DS3)" condition on page 2-141 to appear during loopback setup. The condition clears when you remove the loopback.

Step 8 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-9.

Test and Clear the Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Double-click the card to open the card view.

Step 4 Depending upon the card type, click the **Maintenance** > **Loopback** tabs, **Maintenance** > **DS1** tabs, or **Maintenance** > **DS3** tabs.

Step 5 Choose **None** from the Loopback Type column for the port being tested.

Step 6 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty DS-N card, faulty cabling from the DS-N card to the DSx panel or the EIA, or a faulty EIA.

Step 10 Complete the "Test the DS-N Cabling" procedure on page 1-10.

Test the DS-N Cabling

Step 1 Replace the suspected bad cabling (the cables from the test set to the DSx panel or the EIA ports) with a known-good cable.

If a known-good cable is not available, test the suspected bad cable with a test set. Remove the suspected bad cable from the DSx panel or the EIA and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or defective.

Step 2 Resend test traffic on the loopback circuit with a known-good cable installed. If the test set indicates a good circuit, the problem was probably the defective cable.

Step 3 Replace the defective cable.

Step 4 In card view for the DS-N card, depending upon the type, click the **Maintenance** > **Loopback** tabs, **Maintenance** > **DS1** tabs, or **Maintenance** > **DS3** tabs.

Step 5 Choose **None** from the Loopback Type column for the port being tested.

Step 6 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty card or a faulty EIA.

Step 10 Complete the "Test the DS-N Card" procedure on page 1-10.

Test the DS-N Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the Return Materials Authorization (RMA) process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the faulty card.

Step 5 In card view for the DS-N card, depending upon the type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

Step 6 Choose **None** from the Loopback Type column for the port being tested.

Step 7 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 8 Click **Apply**.

Step 9 Click **Yes** in the confirmation dialog box.

Step 10 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty EIA.

Step 11 Complete the "Test the EIA" procedure on page 1-11.

Test the EIA

Step 1 Remove and reinstall the EIA to ensure a proper seating:

- **a.** Remove the lower backplane cover. Loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.
- **b.** Loosen the nine perimeter screws that hold the EIA panel in place.
- **c.** Lift the EIA panel by the bottom to remove it from the shelf assembly.
- **d.** Follow the installation procedure for the appropriate EIA. See the "Replace an Electrical Interface Assembly" procedure on page 3-17.

Step 2 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the reinstalled EIA. If the test set indicates a good circuit, the problem was probably an improperly seated EIA, and you can proceed to Step 16. If the problem persists and the EIA is not shown to be improperly seated, proceed to Step 3.

Step 3 In card view for the DS-N card, depending upon the type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

Step 4 Choose **None** from the Loopback Type column for the port being tested.

Step 5 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 6 Click **Apply**.

Step 7 Click **Yes** in the confirmation dialog box. Proceed to Step 16.

Step 8 If the test set indicates a faulty circuit, the problem is probably a defective EIA. Return the defective EIA to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 9 Replace the faulty EIA. See the "Replace an Electrical Interface Assembly" procedure on page 3-17.

Step 10 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement EIA. If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

Step 11 If the test set indicates a good circuit, the problem was probably the defective EIA. Clear the facility (line) loopback by clicking the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

Step 12 Choose **None** from the Loopback Type column for the port being tested.

Step 13 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 14 Click **Apply**.

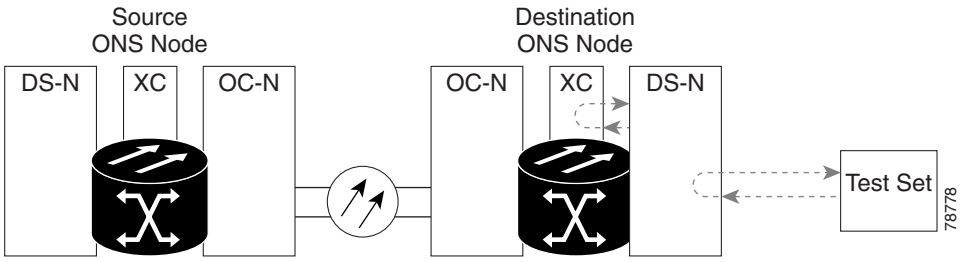
Step 15 Click **Yes** in the confirmation dialog box.

Step 16 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12.

1.3.6 Perform a Hairpin Test on a Destination Node Port (East to West)

The hairpin test is performed on the cross-connect card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through the card isolates the possibility that the cross-connect card is the cause of the faulty circuit. Figure 1-15 shows an example of a hairpin loopback on a destination node port.

Figure 1-15 Hairpin on a Destination Node Port



Note The ONS 15454 does not support simplex operation on the XC10G cross-connect card. Two cross-connect cards of the same type must be installed for each node.

Create the Hairpin Circuit on the Destination Node Port

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

- **a.** If you just completed the "Perform a Facility (Line) Loopback on a Source DS-N Port (West to East)" procedure on page 1-8, leave the electrical test set hooked up to the DS-N port in the destination node.
- **b.** If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. The Tx and Rx terminals connect to the same port.
- **c.** Adjust the test set accordingly.

Step 2 Use CTC to set up the hairpin circuit on the test port:

- **a.** In node view, click the **Circuits** tab and click **Create**.
- **b.** In the Circuit Creation dialog box, choose the type and size, such as an STS-1.
- **c.** Click **Next**.
- **d.** In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "Hairpin1."
- **e.** Uncheck the **Bidirectional** check box.
- **f.** Click **Next**.
- **g.** In the Circuit Creation source dialog box, select the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.
- **h.** Click **Next**.
- **i.** In the Circuit Creation destination dialog box, use the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) used for the source dialog box.
- **j.** Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab and that the **Dir** column describes it as a one-way circuit.

Step 4 Complete the "Test and Delete the Hairpin Circuit" procedure on page 1-13.

Test and Delete the Hairpin 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 received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the hairpin circuit. Clear the hairpin circuit:

- **a.** Click the **Circuits** tab.
- **b.** Choose the hairpin circuit being tested.
- **c.** Click **Delete**.
- **d.** Click **Yes** in the Delete Circuits dialog box.
- **e.** Confirm that the hairpin circuit is deleted form the Circuits tab list.

Step 4 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18. If the test set indicates a faulty circuit, there might be a problem with the XC10G card.

Step 5 Complete the "Test the Standby XC10G Cross-Connect Card" procedure on page 1-13.

Test the Standby XC10G Cross-Connect Card

Note Two XC10G cross-connect cards (active and standby) must be in use on a node to use this procedure.

Step 1 Perform a reset on the standby XC10G cross-connect card to make it the active card:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

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

Step 2 Initiate an external switching command (side switch) on the cross-connect cards before you retest the loopback circuit:

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby XC10G cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. In the node view, select the **Maintenance** > **Cross-Connect** > **Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active XC10G cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 4 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

Step 5 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 6 To confirm a defective original cross-connect card, complete the "Retest the Original XC10G Cross-Connect Card" procedure on page 1-14.

Retest the Original XC10G Cross-Connect Card

Step 1 Initiate an external switching command (side switch) on the XC10G cross-connect cards:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. In node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. From the Cross-Connect Cards menu, choose **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447) and proceed to Step 4. If the test does not indicate a faulty circuit, proceed to Step 5.

Step 4 Complete the "Replace an In-Service Cross-Connect Card" procedure on page 3-2 for the defective cross-connect card.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

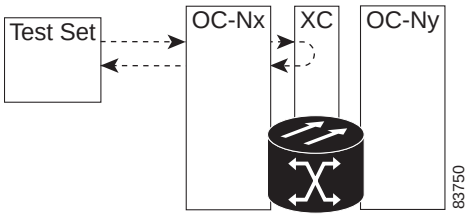
Step 6 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18.

1.3.7 Perform an XC Loopback on a Source Node OC-N STS (East to West)

The XC loopback tests whether any problem exists on the circuit's OC-N span, isolating this span from others present on the card. It also eliminates the cross-connect card as the source of trouble for a faulty circuit. The loopback occurs on the XC10G cross-connect card in a network circuit. Figure 1-16 shows an example of an XC loopback on a source OC-N port.

Note The XC Loopback on an OC-N card does not affect traffic on other circuits.

Figure 1-16 XC Loopback on a Source OC-N Port



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

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

a. If you just completed the "1.5.2 Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" section on page 1-40, 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. The Tx and Rx terminals connect to the same port.

c. Adjust the test set accordingly.

Step 2 Use CTC to put the circuit being tested out of service:

a. In node view, click the **Circuits** tab.

b. Click the circuit and then click **Edit**.

c. In the Edit Circuit dialog box, click the State tab.

d. Choose **OOS-MT** from the Target Circuit State drop-down list.

e. Click **Apply**.

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

Step 3 Use CTC to set up the XC loopback on the circuit being tested:

a. In node view, double-click the OC-N card to open the card view.

b. Click the **Provisioning** > **SONET STS** tabs.

c. Click the check box in the XC Loopback column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog.

Step 4 Complete the "Test the XC Loopback Circuit" procedure on page 1-45.

Test the XC Loopback Circuit

Note This procedure is performed only on OC-N cards.

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the cross-connect. Clear the XC loopback:

a. In card view, click the **Provisioning > SONET STS** tabs.

b. Uncheck the check box in the XC Loopback column for the circuit being tested.

c. Click **Apply**.

d. Click **Yes** in the confirmation dialog.

Step 4 Complete the "Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-48. If the test set indicates a faulty circuit, there might be a problem with the cross-connect card.

Step 5 Complete the "Test the Standby XC10G Cross-Connect Card" procedure on page 1-45.

Test the Standby XC10G Cross-Connect Card

Step 1 Perform a reset on the standby cross-connect card:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

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

Step 2 Initiate an external switching command (side switch) on the cross-connect cards before you retest the loopback circuit:

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. In the node view, select the **Maintenance** > **Cross-Connect** > **Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 4 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

e. Confirm that the XC loopback circuit is deleted form the Circuits tab list. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC10G Cross-Connect Card" procedure on page 1-46.

Retest the Original XC10G Cross-Connect Card

Note This procedure is performed only on OC-N and XC10G cards.

Step 1 Initiate an external switching command (side switch) on the cross-connect cards.

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. In node view, select the **Maintenance** > **Cross-Connect** > **Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447) and proceed to Step 4. If the circuit is not shown to be faulty and the card is not shown to be defective, you are finished with testing.

Step 4 Complete the "Replace an In-Service Cross-Connect Card" procedure on page 3-2 for the defective cross-connect card and perform Step 5.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

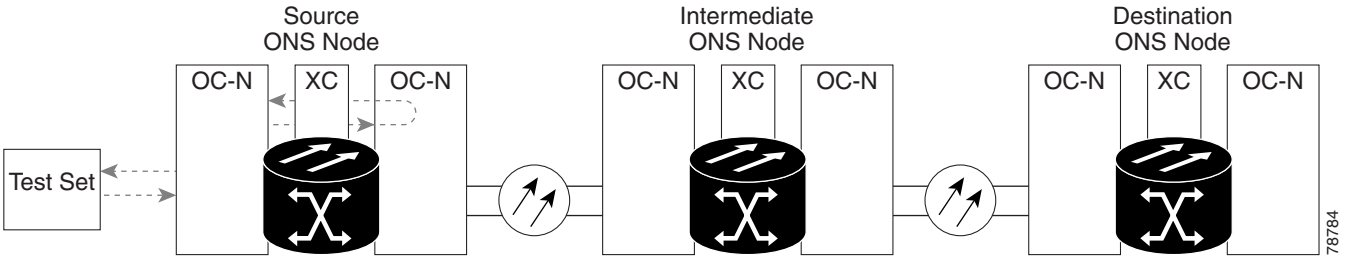
c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

1.3.8 Perform a Terminal (Inward) Loopback on a Source DS-N Port (East to West)

The terminal (inward) loopback test is performed on the node source port in the circuit, such as a source node DS-N port. You first create a bidirectional circuit that starts on the destination node DS-N port and loops back on the source node DS-N port. Then you proceed with the terminal loopback test. Completing a successful terminal loopback to a source node DS-N port verifies that the circuit is good to the source DS-N. Figure 1-17 shows an example of a terminal loopback on a source DS-N port.

Figure 1-17 Terminal (Inward) Loopback on a Source DS-N Port



Caution Performing a loopback on an in-service circuit is service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. For more information about these operations, refer to the *Cisco ONS 15454 Procedure Guide*.

Note DS-3 terminal loopbacks do not transmit an AIS condition in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

Create the Terminal (Inward) Loopback on a Source DS-N Port

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

- **a.** If you just completed the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12, leave the electrical test set hooked up to the DS-N port in the source node.
- **b.** If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. Both Tx and Rx connect to the same port.
- **c.** Adjust the test set accordingly.

Step 2 In CTC node view, click the **Circuits** tab and click **Create**.

Step 3 In the Circuit Creation dialog box, choose the type and size, such as an STS-1.

Step 4 Click **Next**.

Step 5 In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "DS-NtoDS-N."

Step 6 Leave the **Bidirectional** check box checked.

Step 7 Click **Next**.

Step 8 In the Circuit Creation source dialog box, select the **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.

Step 9 Click **Next**.

Step 10 In the Circuit Creation destination dialog box, use the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) used for the source dialog box.

Step 11 Click **Finish**.

Step 12 Confirm that the newly created circuit appears in the **Dir** column as a 2-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)" condition on page 2-144 to appear during a loopback setup. The condition clears when you remove the loopback.

Note DS-3 terminal loopbacks do not transmit a DS-3 AIS (see the "AIS" condition on page 2-21) in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

Step 13 Create the terminal (inward) 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, such as the DS-N card in the destination node.
- **c.** Depending upon the card type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.
- **d.** Select **OOS_MT** from the 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 14 Complete the "Test and Clear the Terminal (Inward) Loopback Circuit on the Destination DS-N Port" procedure on page 1-20.

Test and Clear the Terminal (Inward) Loopback Circuit on the Source DS-N Port

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Double-click the DS-N card in the destination node with the terminal loopback.

Step 4 Depending upon the card type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

Step 5 Select **None** from the Loopback Type column for the port being tested.

Step 6 Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Clear the terminal loopback:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 10 Complete the "Perform a Hairpin Test on a Destination Node Port (East to West)" procedure on page 1-25. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 11 Complete the "Test the Destination DS-N Card" procedure on page 1-21.

Test the Destination DS-N Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the defective DS-N card.

Step 5 Clear the terminal (inward) loopback state on the port:

a. Double-click the DS-N card in the destination node with the terminal loopback.

b. Depending upon the card type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

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

d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 6 Delete the terminal (inward) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

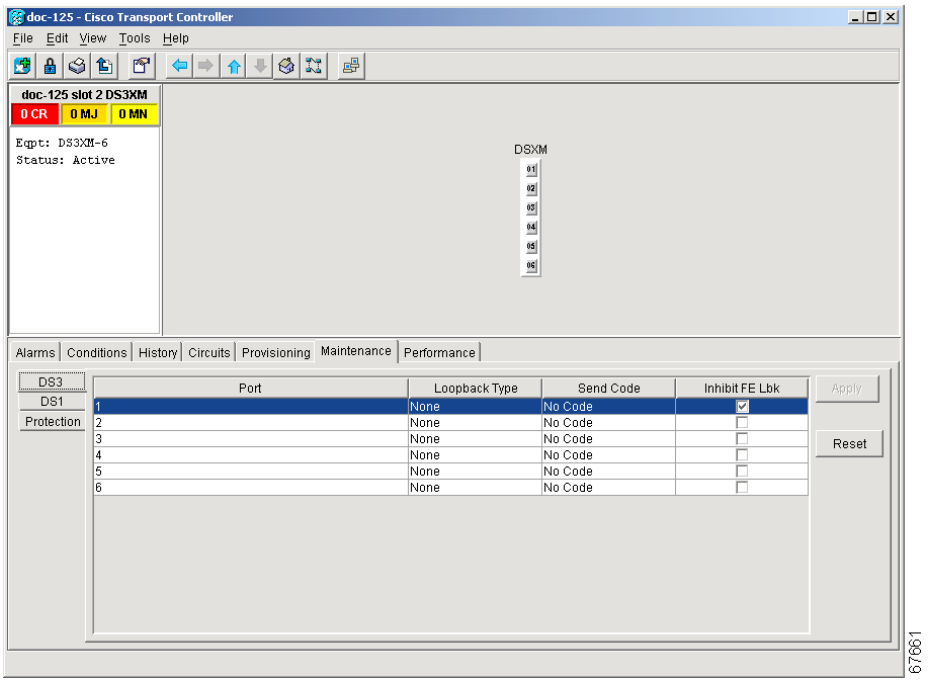
d. Click **Yes** in the Delete Circuits dialog box.

Step 7 Complete the "Perform a Hairpin Test on a Destination Node Port (East to West)" procedure on page 1-25.

1.4 Using the DS3XM-6 Card FEAC (Loopback) Functions

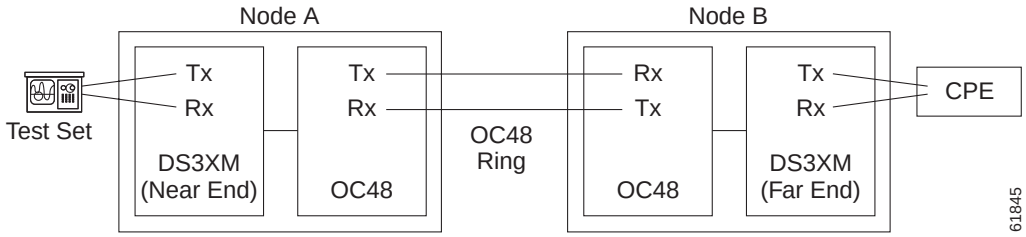
The DS3XM-6 card supports far-end access control (FEAC) functions that are not available on basic DS-3 cards. Click the **Maintenance** tab at the DS3XM-6 card view to reveal the two additional function columns. Figure 1-18 shows the DS3 subtab and the additional Send Code and Inhibit FE Lbk function columns.

Figure 1-18 Accessing FEAC Functions on the DS3XM-6 Card



The “far end” in FEAC refers to the equipment connected to the DS3XM-6 card and not to the far end of a circuit. In Figure 1-19, if a DS3XM-6 (near-end) port is configured to send a Line Loop Code, the code will be sent to the connected test set, not the DS3XM-6 (far-end) port.

Figure 1-19 Diagram of FEAC



1.4.1 FEAC Send Code

The Send Code column on the DS3XM-6 card Maintenance tab only applies to out-of-service (OOS_MT, OOS_AINS) ports configured for CBIT framing. The column lets a user select No Code (the default) or Line Loop Code. Selecting Line Loop Code inserts a line loop activate FEAC in the CBIT overhead transmitting to the connected facility (line). This code initiates a loopback from the facility to the ONS 15454. Selecting No Code sends a line-loop-deactivate FEAC code to the connected equipment, which will remove the loopback. You can also insert a FEAC for the 28 individual DS-1 circuits transmuxed into a DS-3 circuit.

1.4.2 DS-3I Inhibit Loopback

DS-3E and DS-3I cards respond to (but do not send) DS-3-level FEAC codes. You can inhibit FEAC response on ports for these cards using the Inhibit Lbk check box on their Maintenance windows.

1.4.3 DS3XM-6 Inhibit FEAC Loopback

DS3XM-6 ports and transmuxed DS-1s initiate loopbacks when they receive FEAC Line Loop Codes. If the Inhibit FE Lbk check box is checked for a DS-3 port, that port ignores any FEAC Line Loop Codes it receives and will not loop back (return them). Only DS-3 ports can be configured to inhibit FEAC loopback responses; individual DS-1 ports (accessed on the DS3XM DS1 tab) cannot inhibit their responses. If you inhibit a DS-3 port's far end loopback response, this DS-3 port and the DS-1 lines it contains are not restricted from terminal (inward) or facility (line) loopbacks.

1.4.4 FEAC Alarms

When an ONS 15454 port receives an activation code for a FEAC loopback, it raises the LPBKDS1FEAC or LPBKDS3FEAC condition. The condition clears when the port receives the command to deactivate the FEAC loopback. If a node sends a FEAC loopback command to the far end, the sending node raises a LPBKDS1FEAC-CMD or a LPBKDS3FEAC-CMD condition for the port.

1.5 Identify Points of Failure on an Optical Circuit Path

Facility (line) loopbacks, terminal (inward) loopbacks, and cross-connect loopback circuits 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.

You can use these procedures on OC-N cards, G-Series Ethernet cards, transponder (TXP, TXPP) cards, and muxponder (MXP) cards. The example in this section tests an OC-N circuit on a three-node BLSR. Using a series of facility (line) loopbacks and terminal (inward) loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains seven network test procedures:

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

1. A facility (line) loopback on the source node OC-N (or G-Series, TXP, or MXP) port
2. A terminal (inward) loopback on the source node OC-N (or G-Series, TXP, or MXP) port
3. A cross-connect loopback on the source OC-N port
4. A facility (line) loopback on the intermediate node OC-N (or G-Series, TXP, or MXP) port
5. A terminal (inward) loopback on the intermediate node OC-N (or G-Series, TXP, or MXP) port
6. A facility (line) loopback on the destination node OC-N (or G-Series, TXP, or MXP) port
7. A terminal (inward) loopback on the destination node OC-N (or G-Series, TXP, or MXP) port

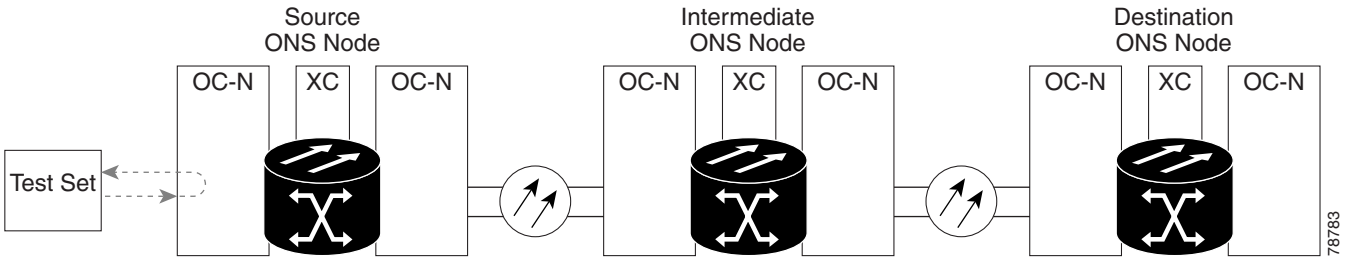
Note All loopback tests require on-site personnel.

1.5.1 Perform a Facility (Line) Loopback on a Source-Node G-Series, MXP, OC-N, or TXP Port

The facility (line) loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source OC-N port in the source node. Completing a successful facility (line) loopback on this port isolates the OC-N port as a possible failure point. Figure 1-20 shows an example of a facility loopback on a circuit source OC-N port. G-Series Ethernet ports, TXPs, and MXPs are tested similarly.

Note Facility (line) loopbacks are not available for G-Series cards prior to software R4.1.

Figure 1-20 Facility (Line) Loopback on a Circuit Source OC-N Port



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

Create the Facility (Line) Loopback on the Source Port

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

Step 2 In CTC node view, double-click the card to open the card view.

Step 3 Click the **Maintenance** > **Loopback** tabs.

Step 4 Choose **OOS_MT** from the State column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

Step 5 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 6 Click **Apply**.

Step 7 Click **Yes** in the confirmation dialog box.

Note It is normal for a "LPBKFACILITY (OCN)" condition on page 2-142, or a "LPBKFACILITY (G1000)" condition on page 2-142 to appear during loopback setup. The condition clears when you remove the loopback.

Step 8 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-39.

Test and Clear the Facility (Line) Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

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

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

c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-40. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-39.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the faulty card.

Step 5 Clear the facility (line) 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 (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 6 Complete the "Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-40.

1.5.2 Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port

The terminal (inward) loopback test is performed on the node source OC-N, G-Series, MXP, or TXP port. For the circuit in this example, it is the source OC-N port in the source node. You first create a bidirectional circuit that starts on the node destination OC-N port and loops back on the node source OC-N port.You then proceed with the terminal loopback test. Completing a successful terminal loopback to a node source port verifies that the circuit is good to the source port. Figure 1-21 shows an example of a terminal loopback on a source OC-N port.

Note Terminal (inward) loopbacks are not available for E-Series Ethernet, ML-Series Ethernet, and DWDM cards in R4.6.

Note Terminal (inward) loopbacks are not available for G-Series cards prior to R4.0.

Figure 1-21 Terminal (Inward) Loopback on a Source-Node OC-N Port

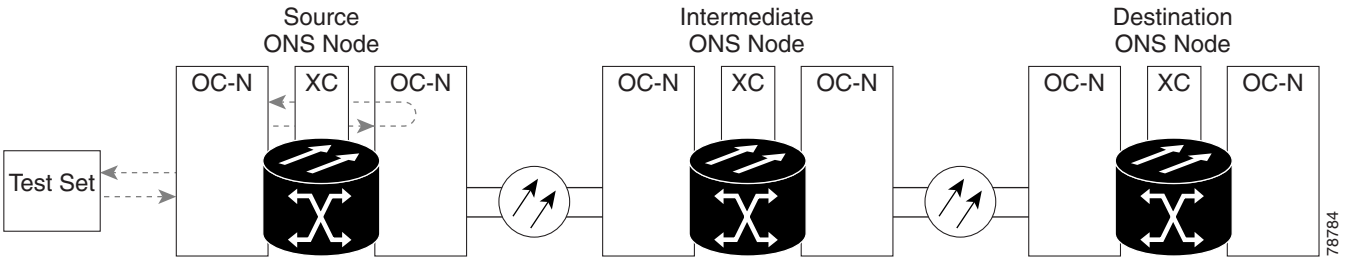
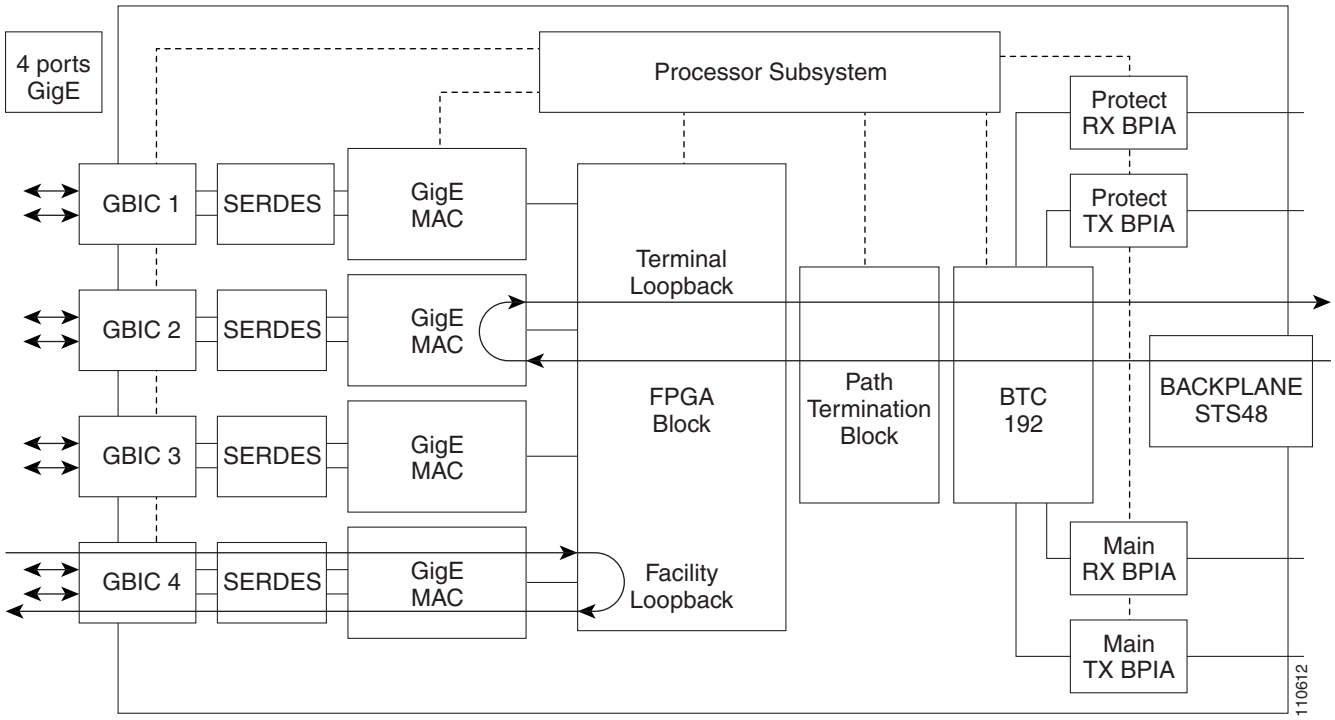


Figure 1-22 shows terminal loopback on a G-Series card.

Figure 1-22 Terminal (Inward) Loopback on a G-Series Port



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

Create the Terminal (Inward) Loopback on a Source Node Port

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

a. If you just completed the "Perform a Facility (Line) Loopback on a Source-Node G-Series, MXP, OC-N, or TXP Port" procedure on page 1-38, leave the optical test set hooked up to the OC-N, G-Series, 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.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal (inward) loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as an STS-1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "OCn1toOCN2."

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) used for the source dialog box.

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)" condition on page 2-144 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the terminal (inward) loopback on the destination port being tested:

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

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

c. Select **OOS_MT** from the State column. If this is a multiport card, select the row appropriate for the desired port.

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

e. Click **Apply**.

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

Step 5 Complete the "Test and Clear the Terminal Loopback Circuit" procedure on page 1-42.

Test and Clear the Terminal Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

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. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 5 Complete the "Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-48. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 6 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-43.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 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. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit before testing the next segment of the network circuit path:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

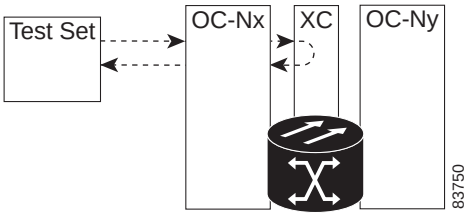
Step 7 Complete the "Create the XC Loopback on the Source OC-N Port" procedure on page 1-44.

1.5.3 Create the XC Loopback on the Source OC-N Port

Note This procedure is only performed on OC-N cards and tests the XC-10G circuit connection.

The cross-connect (XC) loopback test occurs on the XC10G cross-connect card in a network circuit. Completing a successful XC loopback from an OC-N card through the cross-connect card eliminates the cross-connect card as the source of trouble for a faulty circuit. Figure 1-23 shows an example of an XC loopback on a source OC-N port.

Figure 1-23 XC Loopback on a Source OC-N Port



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

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

a. If you just completed the "Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-40, 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. The Tx and Rx terminals connect to the same port.

c. Adjust the test set accordingly.

Step 2 Use CTC to put the circuit being tested out of service:

a. In node view, click the **Circuits** tab.

b. Click the circuit and then click **Edit**.

c. In the Edit Circuit dialog box, click the State tab.

d. Choose **OOS-MT** from the Target Circuit State drop-down list.

e. Click **Apply**.

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

Step 3 Use CTC to set up the XC loopback on the circuit being tested:

a. In node view, double-click the OC-N card to open the card view.

b. Click the **Provisioning** > **SONET STS** tabs.

c. Click the check box in the XC Loopback column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog.

Step 4 Complete the "Test the XC Loopback Circuit" procedure on page 1-45.

Test the XC Loopback Circuit

Note This procedure is performed only on OC-N cards.

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the cross-connect. Clear the XC loopback:

a. In card view, click the **Provisioning** > **SONET STS** tabs.

b. Uncheck the check box in the XC Loopback column for the circuit being tested.

c. Click **Apply**.

d. Click **Yes** in the confirmation dialog.

Step 4 Complete the "Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-48. If the test set indicates a faulty circuit, there might be a problem with the cross-connect card.

Step 5 Complete the "Test the Standby XC10G Cross-Connect Card" procedure on page 1-45.

Test the Standby XC10G Cross-Connect Card

Step 1 Perform a reset on the standby cross-connect card:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

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

Step 2 Initiate an external switching command (side switch) on the cross-connect cards before you retest the loopback circuit:

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. In the node view, select the **Maintenance** > **Cross-Connect** > **Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 4 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

e. Confirm that the XC loopback circuit is deleted form the Circuits tab list. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC10G Cross-Connect Card" procedure on page 1-46.

Retest the Original XC10G Cross-Connect Card

Note This procedure is performed only on OC-N and XC10G cards.

Step 1 Initiate an external switching command (side switch) on the cross-connect cards.

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

b. In node view, select the **Maintenance** > **Cross-Connect** > **Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447) and proceed to Step 4. If the circuit is not shown to be faulty and the card is not shown to be defective, you are finished with testing.

Step 4 Complete the "Replace an In-Service Cross-Connect Card" procedure on page 3-2 for the defective cross-connect card and perform Step 5.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

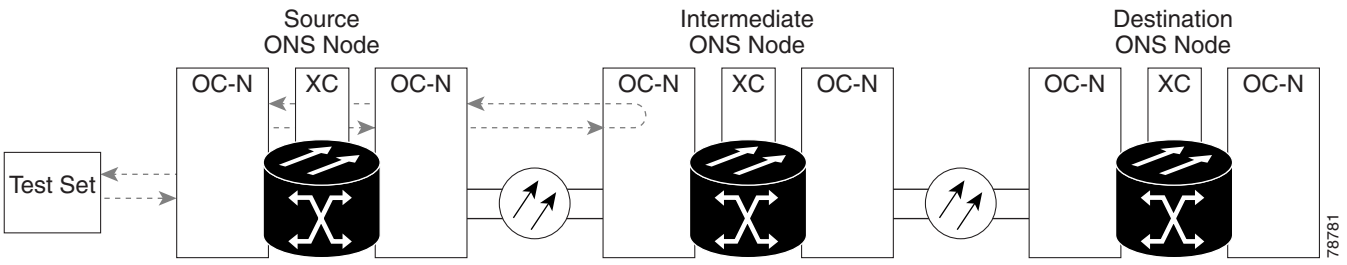
c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

1.5.4 Create a Facility (Line) Loopback on an Intermediate-Node G-Series, MXP, OC-N, or TXP Port

Performing the facility (line) loopback test on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in Figure 1-24, the test is being performed on an intermediate OC-N port.

Figure 1-24 Facility (Line) Loopback on an Intermediate-Node OC-N Port



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

Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

a. If you just completed the "Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-40, 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.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the facility (line) loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as an STS-1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "OCn1toOCn3."

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) used for the source dialog box.

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.

Note It is normal for the "LPBKFACILITY (G1000)" condition on page 2-142, or the "LPBKFACILITY (OCN)" condition on page 2-142 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the facility (line) 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 intermediate node card that requires the loopback.

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

d. Select **OOS_MT** from the 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 5 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-49.

Test and Clear the Facility (Line) Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

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

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

c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 5 Complete the "Create a Terminal Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports" procedure on page 1-51. If the test set indicates a faulty circuit, the problem might be a faulty OC-N card.

Step 6 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-50.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the faulty card.

Step 5 Clear the facility (line) 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 (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

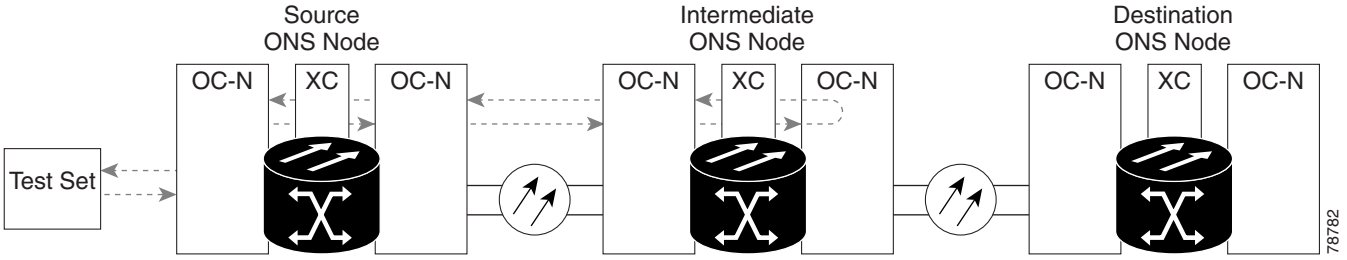
d. Click **Yes** in the Delete Circuits dialog box.

Step 7 Complete the "Create a Terminal Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports" procedure on page 1-51.

1.5.5 Create a Terminal (Inward) Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-25, the terminal loopback is performed on an intermediate OC-N port in the circuit. You first create a bidirectional circuit that originates on the source node OC-N, G-Series, MXP, or TXP port and loops back on the intermediate-node port. You then proceed with the terminal loopback test. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

Figure 1-25 Terminal Loopback on an Intermediate-Node OC-N Port



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

Create a Terminal Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

a. If you just completed the "Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port" section on page 1-48, 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.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal (inward) loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as an STS-1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "OCn1toOCn4."

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) used for the source dialog box.

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list and that it is described in the **Dir** column as a 2-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)" condition on page 2-144 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the terminal loopback on the destination port being tested:

a. Go to the node view of the 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** from the State column. If this is a multiport card, select the row appropriate for the desired port.

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

f. Click **Apply**.

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

Step 5 Complete the "Test and Clear the Terminal Loopback Circuit" procedure on page 1-52.

Test and Clear the Terminal Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

a. Double-click the intermediate node card with the terminal loopback to open the card view.

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

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

d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 5 Complete the "Perform a Facility (Line) Loopback on a Destination-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-54. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 6 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-53.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 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. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

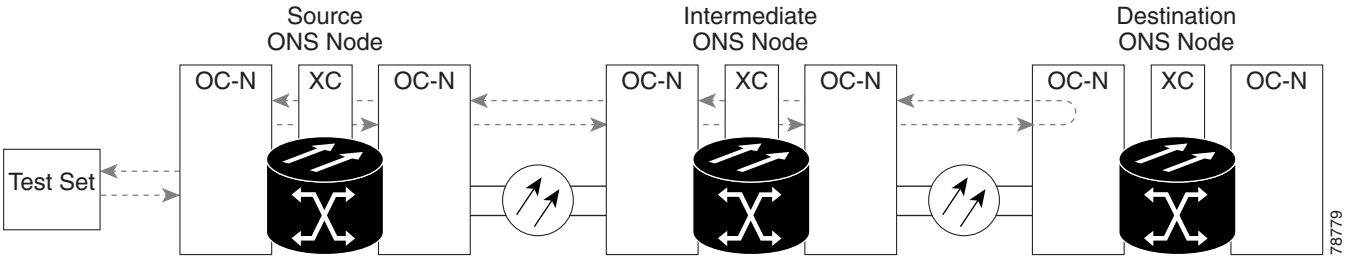
d. Click **Yes** in the Delete Circuits dialog box.

Step 7 Complete the "Perform a Facility (Line) Loopback on a Destination-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-54.

1.5.6 Perform a Facility (Line) Loopback on a Destination-Node OC-N, G-Series, MXP, or TXP Port

You perform a facility (line) loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-26 shows a facility loopback being performed on an OC-N port, but you can also use this procedure on G-Series, MXP, or TXP cards.

Figure 1-26 Facility (Line) Loopback on a Destination Node OC-N Port



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

Create the Facility (Line) Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

a. If you just completed the "Create a Terminal Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports" procedure on page 1-51, 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.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the hairpin circuit on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as an STS-1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "OCn1toOCn5."

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) used for the source dialog box.

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.

Note It is normal for a "LPBKFACILITY (G1000)" condition on page 2-142, or a "LPBKFACILITY (OCN)" condition on page 2-142 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the facility (line) loopback on the destination port being tested:

a. Go to the node view of the destination node:

- Choose **View** > **Go To Other Node** from the menu bar.
- Choose the node from the 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** from the 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 5 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-49.

Test and Clear the Facility (Line) Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

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

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

c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 5 Complete the "Perform a Terminal Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-57. If the test set indicates a faulty circuit, the problem might be a faulty OC-N card.

Step 6 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-50.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the faulty card.

Step 5 Clear the facility (line) 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 (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

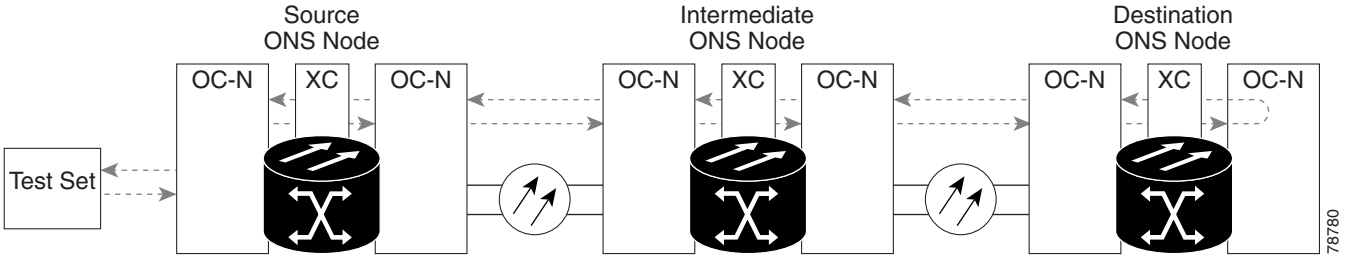
d. Click **Yes** in the Delete Circuits dialog box.

Step 7 Complete the "Perform a Terminal Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-57.

1.5.7 Perform a Terminal Loopback on a Destination Node OC-N, G-Series, 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 1-27 shows a terminal loopback on an intermediate node destination OC-N port.

Figure 1-27 Terminal Loopback on a Destination Node OC-N Port



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

Create the Terminal Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

a. If you just completed the "Perform a Facility (Line) Loopback on a Destination-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-54, 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.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as an STS-1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "OCn1toOCn6."

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) used for the source dialog box.

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)" condition on page 2-144 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the terminal loopback on the destination port being tested:

a. Go to the node view of the destination node:

- Choose **View** > **Go To Other Node** from the menu bar.
- Choose the node from the 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** from the State column. If this is a multiport card, select the row appropriate for the desired port.

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

f. Click **Apply**.

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

Step 5 Complete the "Test and Clear the Terminal Loopback Circuit" procedure on page 1-58.

Test and Clear the Terminal Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

a. Double-click the intermediate node card with the terminal loopback.

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

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

d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

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

Step 5 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 6 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-59.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good card.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 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. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

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

1.6 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.

1.6.1 Restore the Node Database

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

Table 1-2 describes the potential causes of the symptom and the solution.

Table 1-2 Restore the Node Database

Possible Problem	Solution
Incorrect or corrupted node database.	Perform a Restore the Database procedure. Refer to the "Restore the Database" procedure on page 1-60.

Restore the Database

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

Caution E1000-2 cards lose traffic for approximately 90 seconds when an ONS 15454 database is restored. Traffic is lost during the period of spanning tree reconvergence. The CARLOSS (E100T, E1000F) alarm appears and clears during this period.

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

Step 1 In CTC, log into the node where you will restore the database:

a. On the PC connected to the ONS 15454, start Netscape or Internet Explorer.

b. In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15454 IP address.

A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to an ONS 15454, this process can take several minutes. After the download, the CTC Login dialog box appears.

c. In the Login dialog box, type a user name and password (both are case sensitive) and click **Login**. The CTC node view window appears.

Step 2 Ensure that no ring or span (four-fiber only) switch events are present; for example, ring-switch east or west and span-switch east or west. In network view, click the **Conditions** tab and click **Retrieve** to view a list of conditions.

Step 3 If switch events need to be cleared, in node view click the **Maintenance > BLSR** tabs and view the West Switch and East Switch columns.

a. If a switch event (not caused by a line failure) is present, choose **CLEAR** from the drop-down menu and click **Apply**.

b. If a switch event caused by the Wait to Restore (WTR) condition is present, choose **LOCKOUT SPAN** from the drop-down menu and click **Apply**. When the LOCKOUT SPAN is applied, choose **CLEAR** from the drop-down menu and click **Apply**.

Step 4 In node view, click the **Maintenance > Database** tabs.

Step 5 Click **Restore**.

Step 6 Locate the database file stored on the workstation hard drive or on network storage.

Note To clear all existing provisioning, locate and upload the database found on the latest ONS 15454 software CD.

Step 7 Click the database file to highlight it.

Step 8 Click **Open**. The DB Restore dialog box appears. Opening a restore file from another node or from an earlier backup might affect traffic on the login node.

Step 9 Click **Yes**.

The Restore Database dialog box monitors the file transfer.

Step 10 Wait for the file to complete the transfer to the TCC2.

Step 11 Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears. Wait for the node to reconnect.

Step 12 If you cleared a switch in Step 3, reapply the switch as needed.

1.6.2 Restore the Node to Factory Configuration

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

Table 1-3 describes the possible problems and the solution.

Table 1-3 Restore the Node to Factory Configuration

Possible Problem	Solution
Failure of both TCC2 cards in the node.	Restore the node to factory configuration. Refer to the "Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" procedure on page 1-63 or the "Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" procedure on page 1-64 as required.
Replacement of both TCC2 cards at the same time.	

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

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

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

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

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

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

Note If the software package files and database backup files are located in different directories, complete the Package and Database fields (Figure 1-28 on page 1-63).

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

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

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

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

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

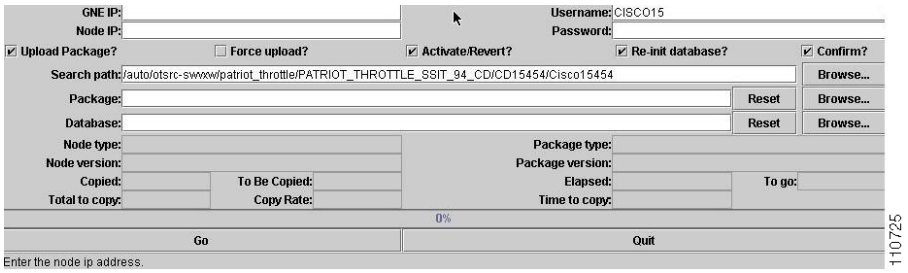
Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 To find the recovery tool file, go to **Start > Run > Browse** and select the CD drive.

Step 3 On the CD drive, go to the CISCO15454 folder and choose **All Files from the Files of Type** drop-down menu.

Step 4 Select the RE-INIT.jar file and click **Open** to open the reinit tool (Figure 1-28).

Figure 1-28 Reinitialization Tool in Windows



Step 5 If the node you are reinitializing is an external network element (ENE) in a proxy server network, enter the IP address of the gateway network element (GNE) in the GNE IP field. If not, leave it blank.

Step 6 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-28).

Step 7 If the User ID field does not contain your user ID, enter the ID. Enter your password in the Password field.

Step 8 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If one is not checked, check the check box.

Step 9 If you are uploading the same version of software that is already active (for example, you are trying to upload version 4.6 when version 4.6 is already active), check the Force Upload checkbox.This option forces the NE to have the same software version on the working and protect flash memory.

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

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

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

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

Step 12 Click **Yes**.

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

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

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

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

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

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

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

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

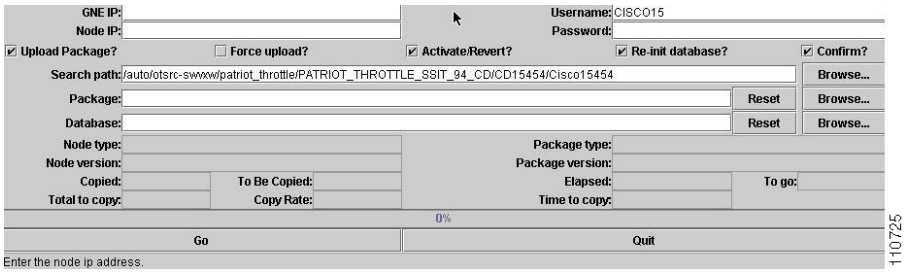
Note Java Runtime Environment (JRE) 1.03_02 must also be installed on the computer you use to perform this procedure.

Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 To find the recovery tool file, go to the CISCO15454 directory on the CD (usually /cdrom/cdrom0/CISCO15454).

Step 3 If you are using a file explorer, double-click the **RE-INIT.jar** file to open the reinit tool (Figure 1-29). If you are working with a command line interface, run **java -jar RE-INIT.jar**.

Figure 1-29 Reinitialization Tool in UNIX



Step 4 If the node you are reinitializing is an ENE in a proxy server network, enter the IP address of the GNE in the GNE IP field. If not, leave it blank.

Step 5 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-29).

Step 6 If the User ID field does not contain your user ID, enter the ID. Enter your password in the Password field.

Step 7 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If one is not checked, check the check box.

Step 8 If you are uploading the same version of software that is already active (for example, you are trying to upload version 4.6 when version 4.6 is already active), check the Force Upload checkbox. This option forces the NE to have the same software version on the working and protect flash memory.

Step 9 In the Search Path field, verify that the path to the CISCO15454 folder on the CD-ROM drive is listed.

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

Step 10 Click **Go**. A confirmation dialog box appears.

Step 11 Click **Yes**.

Step 12 The status bar at the bottom of the screen displays Complete when the node has activated the software and uploaded the database.

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

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

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

1.7 PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and JREs for R4.6, and troubleshooting procedures for PC and network connectivity to the ONS 15454.

1.7.1 PC System Minimum Requirements

Workstations running CTC R4.6 for the ONS products on Windows platforms need to have the following minimum requirements:

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

1.7.2 Sun System Minimum Requirements

Workstations running CTC R4.6 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

1.7.3 Supported Platforms, Browsers, and JREs

Software R4.6 CTC supports the following platforms:

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

Software R4.6 CTC supports the following browsers and JREs:

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

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

Note You can obtain browsers at the following URLs:
Netscape: http://channels.netscape.com/ns/browsers/default.jsp
Internet Explorer: http://www.microsoft.com

Note The recommended JRE version is JRE 1.4.2.

Note JRE 1.4.2 for Windows and Solaris is available on R4.6 product CDs.

1.7.4 Unsupported Platforms and Browsers

Software R4.6 does not support the following platforms:

- Windows 95
- Solaris 2.5
- Solaris 2.6

Software R4.6 does not support the following browsers and JREs:

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

1.7.5 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.

Table 1-4 on page 1-67 describes the possible problems and the solutions.

Table 1-4 Unable to Verify the IP Configuration of Your PC

Possible Problem	Solution
The IP address was typed incorrectly.	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 1-68.
The IP configuration of your PC is not properly set.	Verify the IP configuration of your PC. Complete the "Verify the IP Configuration of Your PC" procedure on page 1-68. If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC.

Verify the IP Configuration of Your PC

Step 1 Open a DOS command window by selecting **Start > Run** from the Start menu.

Step 2 In the Open field, type **command** and then click **OK**. The DOS command window appears.

Step 3 At the prompt in the DOS window, type one of the following commands:

- For Windows 98, NT, and 2000, type **ipconfig** and press the **Enter** key.

The Windows IP configuration information appears, including the IP address, subnet mask, and the default gateway.

Note The winipcfg command only returns the information above if you are on a network.

Step 4 At the prompt in the DOS window, type **ping** followed by the IP address shown in the Windows IP configuration information previously displayed.

Step 5 Press the **Enter** key to execute the command.

If the DOS window returns multiple (usually four) replies, the IP configuration is working properly.

If you do not receive a reply, your IP configuration might not be properly set. Contact your Network Administrator for instructions to correct the IP configuration of your PC.

1.7.6 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.

Table 1-5 describes the possible problem and the solution.

Table 1-5 Browser Login Does Not Launch Java

Possible Problem	Solution
The PC operating system and browser are not properly configured.	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 1-68 and the "Reconfigure the Browser" procedure on page 1-69.

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. On 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. On 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, **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** on the Preferences window and exit the browser.

Step 3 If you are using Internet Explorer:

a. On 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 "1.8.3 Browser Stalls When Downloading CTC JAR Files From TCC2" section on page 1-74.

Step 5 Verify that the computer does not have two network interface cards (NICs) installed. If the computer does have two NICs, remove one.

Step 6 Restart the browser and log on to the ONS 15454.

1.7.7 Unable to Verify the NIC Connection on Your PC

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

Table 1-6 describes the possible problems and the solutions.

Table 1-6 Unable to Verify the NIC Connection on your PC

Possible Problem	Solution
The CAT-5 cable is not plugged in properly.	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.
The CAT-5 cable is damaged.	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.
Incorrect type of CAT-5 cable is being used.	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 "1.10.2.1 Crimp Replacement LAN Cables" section on page 1-97.
The NIC is improperly inserted or installed.	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.
The NIC is faulty.	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.

1.7.8 Verify PC Connection to the ONS 15454 (ping)

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

Table 1-7 describes the possible problem and the solution.

Table 1-7 Verify PC Connection to ONS 15454 (ping)

Possible Problem	Solution
A lost connection between the PC and the ONS 15454.	Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 TCC2 card. A ping command should work if the PC connects directly to the TCC2 card or uses a LAN to access the TCC2 card. Complete the "Ping the ONS 15454" procedure on page 1-71.

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**, type **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 type:

```
ping ONS-15454-IP-address
```

For example:

```
ping 198.168.10.10
```

Step 3 If the workstation has connectivity to the ONS 15454, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a "Request timed out" message appears.

Step 4 If the ping is successful, an active TCP/IP connection exists. Restart CTC.

Step 5 If the ping is not successful, and the workstation connects to the ONS 15454 through a LAN, check that the workstation's IP address is on the same subnet as the ONS node.

Step 6 If the ping is not successful and the workstation connects directly to the ONS 15454, check that the link light on the workstation's NIC is illuminated.

1.7.9 The IP Address of the Node is Unknown

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

Table 1-8 describes the possible problem and the solution.

Table 1-8 Retrieve the Unknown IP Address of the Node

Possible Problem	Solution
The node is not set to the default IP address.	Leave one TCC2 card in the shelf. Connect a PC directly to the remaining TCC2 card and perform a hardware reset of the card. The TCC2 card transmits the IP address after the reset to enable you to capture the IP address for login. Complete the "Retrieve Unknown Node IP Address" procedure on page 1-71.

Retrieve Unknown Node IP Address

Step 1 Connect your PC directly to the active TCC2 card Ethernet port on the faceplate.

Step 2 Start the Sniffer application on your PC.

Step 3 Perform a hardware reset by pulling and reseating the active TCC2 card.

Step 4 After the TCC2 card completes resetting, it broadcasts its IP address. The Sniffer software on your PC will capture the IP address being broadcast.

1.8 CTC Operation Troubleshooting

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

1.8.1 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.

Table 1-9 describes the possible problem and the solution.

Table 1-9 Unable to Launch CTC Help After Removing Netscape

Possible Problem	Solution
Loss of association between browser and Help files.	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 1-72 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.

1.8.2 Unable to Change Node View to Network View

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

Table 1-10 describes the possible problem and the solution.

Table 1-10 Browser Stalls When Downloading Files From TCC2

Possible Problem	Solution
The large, multinode BLSR requires more memory for the graphical user interface (GUI) environment variables.	Reset the system or user CTC_HEAP environment variable to increase the memory limits. Complete the "Reset the CTC_HEAP Environment Variable for Windows" procedure on page 1-73 or the "Reset the CTC_HEAP Environment Variable for Solaris" procedure on page 1-73 to enable the CTC_HEAP variable change. **Note** This problem typically affects large networks where additional memory is required to manage large numbers of nodes and circuits.

Reset the CTC_HEAP Environment Variable for Windows

Step 1 Exit any and all open and running CTC and Netscape applications.

Step 2 From the Windows Desktop, right-click My Computer and choose **Properties** in the shortcut menu.

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

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

Step 5 Click **New** under the User variables field or the System variables field.

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

Step 7 Type **256** in the Variable Value field, and then click **OK** to create the variable.

Step 8 Click **OK** in the Environment Variables window to accept the changes.

Step 9 Click **OK** in the System Properties window to accept the changes.

Restart the browser and CTC software.

Reset the CTC_HEAP Environment Variable for Solaris

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

Step 2 Kill any Netscape applications.

Step 3 In the user shell window, set the environment variable to increase the heap size:

```
% setenv CTC_HEAP 256
```

Step 4 Restart the browser and CTC software in the same user shell window.

1.8.3 Browser Stalls When Downloading CTC JAR Files From TCC2

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

Table 1-11 describes the possible problem and the solution.

Table 1-11 Browser Stalls When Downloading JAR Files from TCC2

Possible Problem	Solution
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.	Disable the VirusScan Download Scan feature. Complete the "Disable the VirusScan Download Scan" procedure on page 1-74.

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.

1.8.4 CTC Does Not Launch

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

Table 1-12 describes the possible problem and the solution.

Table 1-12 CTC Does Not Launch

Possible Problem	Solution
The Netscape browser cache might point to an invalid directory.	Redirect the Netscape cache to a valid directory. Complete the "Redirect the Netscape Cache to a Valid Directory" procedure on page 1-75.

Redirect the Netscape Cache to a Valid Directory

Step 1 Launch Netscape.

Step 2 open the **Edit** menu.

Step 3 Choose **Preferences**.

Step 4 Under the Category column on the left side, expand the **Advanced** category and choose the **Cache** tab.

Step 5 Change your disk cache folder to point to the cache file location.

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

1.8.5 Slow CTC Operation or Login Problems

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

Table 1-13 describes the possible problem and the solution.

Table 1-13 Slow CTC Operation or Login Problems

Possible Problem	Solution
The CTC cache file might be corrupted or might need to be replaced.	Delete the CTC cache file. This operation forces the ONS 15454 to download a new set of JAR files to your computer hard drive. Complete the "Delete the CTC Cache File Automatically" procedure on page 1-75 or the "Delete the CTC Cache File Manually" procedure on page 1-76.

Delete the CTC Cache File Automatically

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

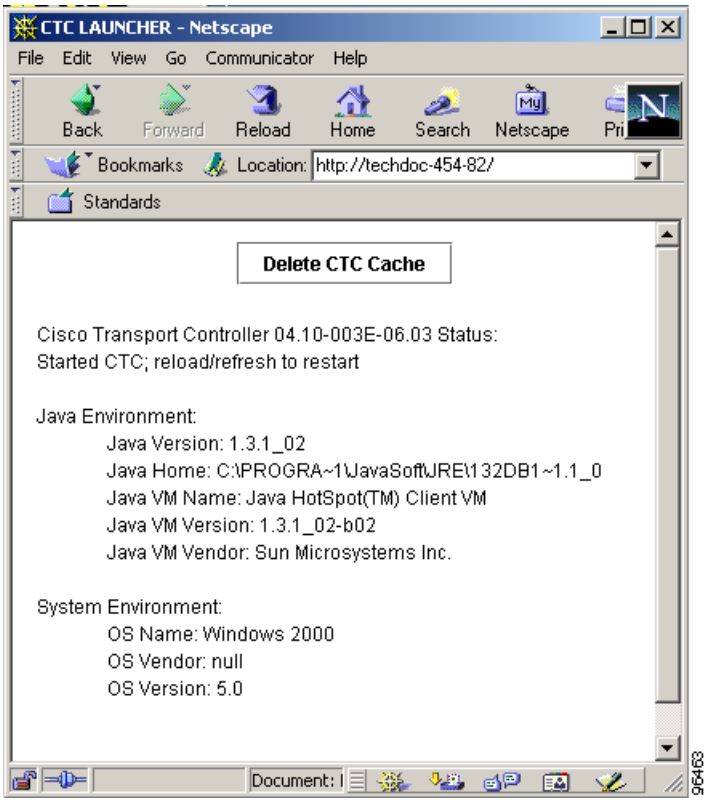
Step 1 Enter an ONS 15454 IP address into the browser URL field. The initial browser window shows a **Delete CTC Cache** button.

Step 2 Close all open CTC sessions and browser windows. The PC operating system does not allow you to delete files that are in use.

Step 3 Click **Delete CTC Cache** on the initial browser window to clear the CTC cache. Figure 1-30 shows the Delete CTC Cache window.

Note For CTC releases earlier than R3.0, automatic deletion is unavailable. For CTC cache file manual deletion, complete the "Delete the CTC Cache File Manually" procedure on page 1-76.

Figure 1-30 Deleting the CTC Cache



Delete the CTC Cache File Manually

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

Step 1 To delete the JAR files manually, from the Windows Start menu choose **Search > For Files or Folders**.

Step 2 Enter *.jar in the Search for files or folders named field in the Search Results dialog box and click **Search Now**.

Step 3 Click the **Modified** column in the Search Results dialog box to find the JAR files that match the date when you downloaded the files from the TCC2. These files might include CTC*.jar, CMS*.jar, and jar_cache*.tmp.

Step 4 Highlight the files and press the keyboard **Delete** key.

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

1.8.6 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.

Table 1-14 describes the possible problems and the solutions.

Table 1-14 Node Icon is Gray on CTC Network View

Possible Problem	Solution
Different CTC releases not recognizing each other.	Correct the core version build as described in the "1.8.9 Different CTC Releases Do Not Recognize Each Other" section on page 1-80.
A username/password mismatch.	Correct the username and password as described in the "1.8.10 Username or Password Do Not Match" section on page 1-81.
No IP connectivity between nodes.	Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.8.15 Ethernet Connections" section on page 1-83.
A lost DCC connection.	Usually accompanied by an embedded operations channel (EOC) alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm.

1.8.7 CTC Cannot Launch Due to Applet Security Restrictions

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

Table 1-15 on page 1-78 describes the possible problem and the solution.

Table 1-15 CTC Cannot Launch Due to Applet Security Restrictions

Possible Problem	Solution
You are logging into a node running CTC Software R4.0 or earlier. Releases earlier than R4.1 require a modification to the java.policy file so that CTC JAR files can be downloaded to the computer. The modified java.policy file might not exist on the computer.	1. Install the software CD for the release of the node you are logging into. 2. Run the CTC Setup Wizard (double-click **Setup.exe**). 3. Choose **Custom installation**, then choose the Java Policy option. For additional information, refer to the CTC installation information in the *Cisco ONS 15454 Procedure Guide*. 4. If the software CD is not available, you must manually edit the java.policy file on your computer. Complete the "Manually Edit the java.policy File" procedure on page 1-78.

Manually Edit the java.policy File

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

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

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

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

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

Step 4 Save the file and restart Netscape.

CTC should now start correctly.

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

1.8.8 Java Runtime Environment Incompatible

Symptom The CTC application does not run properly.

Table 1-16 describes the possible problem and the solution.

Table 1-16 Java Runtime Environment Incompatible

Possible Problem	Solution
The compatible Java 2 JRE is not installed.	The JRE contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language. The ONS 15454 CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD and on the Cisco ONS 15454 documentation CD. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-79. 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 1-17 shows JRE compatibility with ONS 15454 software releases.

Table 1-17 JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15454 R2.2.1 and earlier	Yes	No	No
ONS 15454 R2.2.2	Yes	Yes	No
ONS 15454 R3.0	Yes	Yes	No
ONS 15454 R3.1	Yes	Yes	No
ONS 15454 R3.2	Yes	Yes	No
ONS 15454 R3.3	Yes	Yes	No
ONS 15454 R3.4	No	Yes	No
ONS 15454 R4.0[1]	No	Yes	No
ONS 15454 R4.1	No	Yes	No
ONS 15454 R4.5	No	Yes	No
ONS 15454 R4.6	No	Yes	Yes

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

Launch CTC to Correct the Core Version Build

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

Step 2 Start the browser.

Step 3 Type the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged in with or an IP address other than the original.

Step 4 Log into CTC. The browser downloads the JAR file from CTC.

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

1.8.9 Different CTC Releases Do Not Recognize Each Other

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

Table 1-18 describes the possible problem and the solution.

Table 1-18 Different CTC Releases Do Not Recognize Each Other

Possible Problem	Solution
The software loaded on the connecting workstation and the software on the TCC2 card are incompatible.	This occurs when the TCC2 software is upgraded but the PC has not yet upgraded the compatible CTC JAR file. It also occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version. **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. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-80.

Launch CTC to Correct the Core Version Build

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

Step 2 Start the browser.

Step 3 Type the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.

Step 4 Log into CTC. The browser downloads the JAR file from CTC.

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

1.8.10 Username or Password Do Not Match

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

Table 1-19 describes the possible problem and the solution.

Table 1-19 Username or Password Do Not Match

Possible Problem	Solution
The username or password entered does not match the information stored in the TCC2.	All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes. For initial login to the ONS 15454, type the CISCO15 user name in capital letters and click **Login** (no password is required). If you are using a CTC Software R2.2.2 or earlier and CISCO15 does not work, type cerent454 for the user name. Complete the "Verify Correct Username and Password" procedure on page 1-81.

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 TAC (1 800 553-2447) to have them enter your system and create a new user name and password.

1.8.11 No IP Connectivity Exists Between Nodes

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

Table 1-20 describes the possible problem and the solution.

Table 1-20 No IP Connectivity Exists Between Nodes

Possible Problem	Solution
A lost Ethernet connection.	Usually is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.8.15 Ethernet Connections" section on page 1-83.

1.8.12 DCC Connection Lost

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

Table 1-21 describes the possible problem and the solution.

Table 1-21 DCC Connection Lost

Possible Problem	Solution
A lost DCC connection.	Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm.

1.8.13 "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.

Table 1-22 describes the possible problem and the solution.

Table 1-22 "Path in Use" Error When Creating a Circuit

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

1.8.14 Calculate and Design IP Subnets

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

Table 1-23 describes the possible problem and the solution.

Table 1-23 Calculate and Design IP Subnets

Possible Problem	Solution
The IP capabilities of the ONS 15454 require specific calculations to properly design IP subnets.	Cisco provides a free online tool to calculate and design IP subnets. Go to http://www.cisco.com/techtools/ip_addr.html. For information about ONS 15454 IP capability, refer to the *Cisco ONS 15454 Reference Manual.*

1.8.15 Ethernet Connections

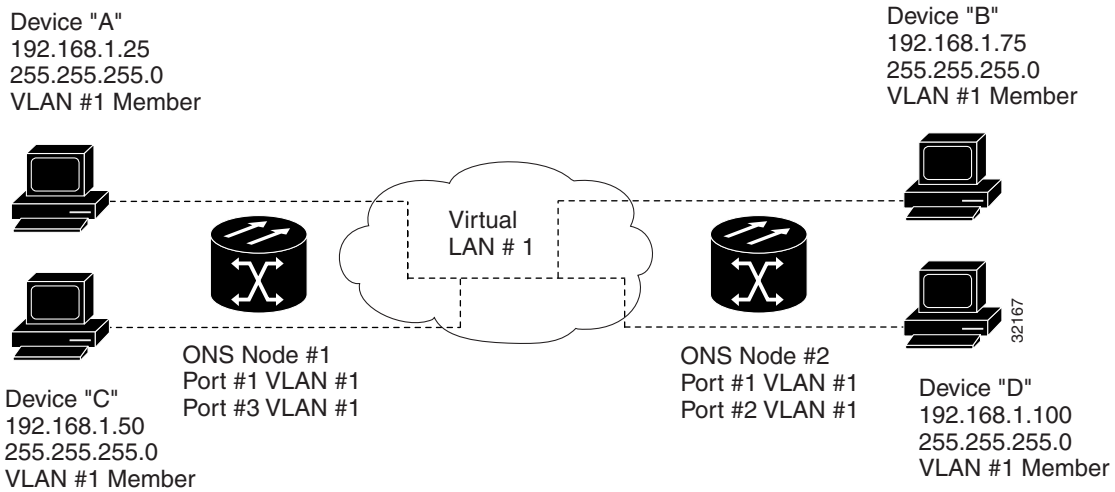
Symptom Ethernet connections appear to be broken or are not working properly.

Table 1-24 describes the possible problem and the solution.

Table 1-24 Calculate and Design IP Subnets

Possible Problem	Solution
Improperly seated connections.	You can fix most connectivity problems in an Ethernet network by following a few guidelines. See Figure 1-31 when using the steps in the "Verify Ethernet Connections" procedure on page 1-84.
Incorrect connections.	

Figure 1-31 Ethernet Connectivity Reference



Verify Ethernet Connections

Step 1 Verify that the alarm filter is turned OFF.

Step 2 Check for SONET and dense wavelength division multiplexing (DWDM) alarms on the STS-N that carries the VLAN #1 Ethernet circuit. Clear any alarms by looking them up in Chapter 2, "Alarm Troubleshooting."

Step 3 Check for Ethernet-specific alarms. Clear any raised alarms by looking up that alarm in Chapter 2, "Alarm Troubleshooting."

Step 4 Verify that the ACT LED on the Ethernet card is green.

Step 5 Verify that Ports 1 and 3 on ONS 15454 #1 and Ports 1 and 2 on ONS 15454 #2 have green link-integrity LEDs illuminated.

Step 6 If no green link-integrity LED is illuminated for any of these ports:

- **a.** Verify physical connectivity between the ONS 15454s and the attached device.
- **b.** Verify that the ports are enabled on the Ethernet cards.
- **c.** Verify that you are using the proper Ethernet cable and that it is wired correctly, or replace the cable with a known-good Ethernet cable.
- **d.** Check the status LED on the Ethernet card faceplate to ensure the card booted up properly. This LED should be steady green. If necessary, remove and reinsert the card and allow it to reboot.
- **e.** It is possible that the Ethernet port is functioning properly but the link LED itself is broken. Complete the "Verify Card LED Operation" procedure on page 1-105.

Step 7 Verify connectivity between device A and device C by pinging between these locally attached devices. Complete the "Verify PC Connection to the ONS 15454 (ping)" procedure on page 1-70. If the ping is unsuccessful:

- **a.** Verify that device A and device C are on the same IP subnet.
- **b.** open the Ethernet card in CTC card view and click the **Provisioning** > **VLAN** tabs to verify that both Port 1 and Port 3 on the card are assigned to the same VLAN.
- **c.** If a port is not assigned to the correct VLAN, click that port column in the VLAN row and set the port to Tagged or Untag. Click **Apply**.

Step 8 Repeat Step 7 for devices B and D.

Step 9 Verify that the Ethernet circuit that carries VLAN #1 is provisioned and that ONS 15454 #1 and ONS 15454 #2 ports also use VLAN #1.

1.8.16 VLAN Cannot Connect to Network Device from Untag Port

Symptom Networks that have a VLAN with one ONS 15454 Ethernet card port set to Tagged and one ONS 15454 Ethernet card set to Untag might have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port (Figure 1-32). They might also see a higher than

normal runt packets count at the network device attached to the Untag port. This symptom/limitation also exists when ports within the same card or ports within the same chassis are put on the same VLAN, with a mix of tagged and untagged.

Figure 1-32 VLAN with Ethernet Ports at Tagged and Untag

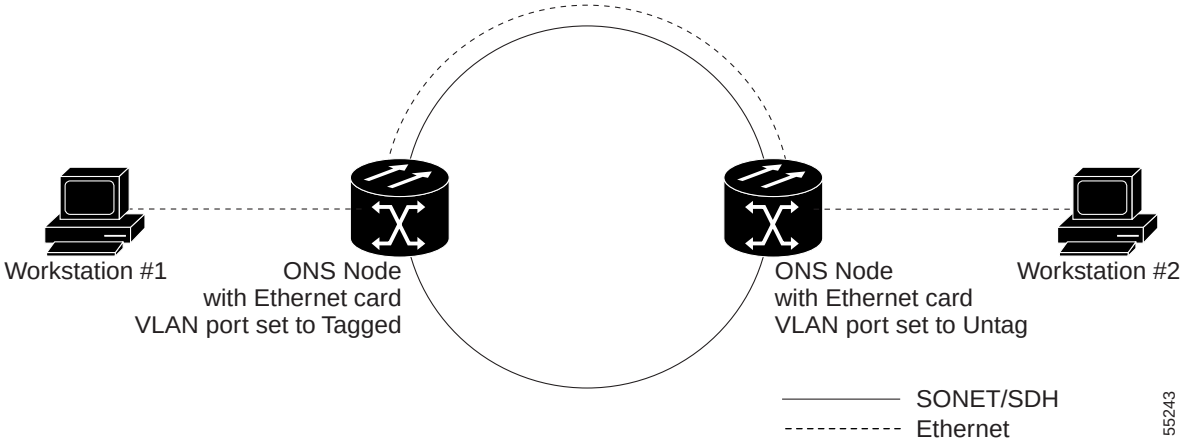


Table 1-25 describes the possible problems and the solution.

Table 1-25 Verify VLAN Connection to Network Device from Untag Port

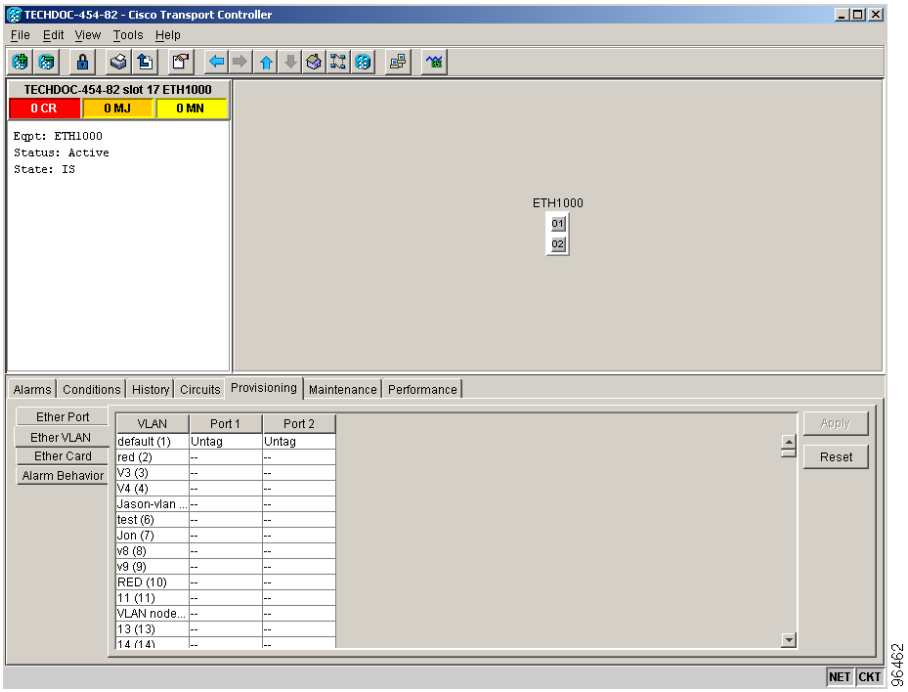
Possible Problem	Solution
The Tagged ONS 15454 adds the IEEE 802.1Q tag and the Untag ONS 15454 removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet.	The solution is to set both ports in the VLAN to Tagged to stop the stripping of the 4 bytes from the data packet and prevent the NIC card in the network access device from recognizing the packet as a runt and dropping it. Network devices with IEEE 802.1Q-compliant NIC cards accept the tagged packets. Network devices with non IEEE 802.1Q compliant NIC cards still drop these tagged packets. The solution might require upgrading network devices with non-IEEE 802.1Q compliant NIC cards to IEEE 802.1Q compliant NIC cards. You can also set both ports in the VLAN to Untag, but you will lose IEEE 802.1Q compliance.
Dropped packets can also occur when ARP attempts to match the IP address of the network device attached to the Untag port with the physical MAC address required by the network access layer.	

Change VLAN Port Tag and Untagged Settings

Step 1 Display the CTC card view for the Ethernet card involved in the problem VLAN.

Step 2 Click the **Provisioning > Ether VLAN** tabs (Figure 1-33).

Figure 1-33 Configuring VLAN Membership for Individual Ethernet Ports



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

Step 4 At the VLAN port set to Untag, click the port and choose **Tagged**.

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

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

1.8.17 Cross-Connect Card Oscillator Fails

Symptom: The XC or XCVT card can be affected by this problem. (In R4.6, the XC10G card automatically detects it.) It is indicated by a CTNEQPT-PBPROT or CTNEQPT-PBWORK condition raised against all I/O cards in the node. The following conditions might also be raised on the node:

- SWMTXMOD against one or both cross-connect cards
- SD-L against near-end or far-end line cards
- AIS-L against far-end line cards
- RFI-L against near-end line cards

Table 1-26 describes the potential cause(s) of the symptom and the solution(s).

Table 1-26 Cross-Connect Card Oscillator Fails

Possible Problem	Solution
The XC or XCVT card has oscillator failure.	1. If the Slot 8 cross-connect card is active, see the "1.8.17.1 Resolve the XC Oscillator Failure When Slot 8 XC Card is Active" section on page 1-87. 2. If the Slot 10 cross-connect card is active, see the "1.8.17.2 Resolve the XC Oscillator Failure When Slot 10 XC Card is Active" section on page 1-87.

1.8.17.1 Resolve the XC Oscillator Failure When Slot 8 XC Card is Active

Step 1 If the CTNEQPT-PBPROT condition is reported against all I/O cards in the node and the Slot 8 cross-connect card is active, right-click the Slot 10 cross-connect card.

Step 2 Choose **Reset Card,** then click **OK**. (Slot 8 remains active and Slot 10 remains standby.)

Step 3 If the alarm remains, reseat the Slot 10 card.

Step 4 If CTNEQPT-PBPROT does not clear, replace the Slot 10 cross-connect card with a spare card.

Step 5 If CTNEQPT-PBPROT does not clear, replace the spare card placed in Slot 10 with the original cross-connect card.

Step 6 Right-click the Slot 8 card and choose **Reset Card**.

Step 7 Click **OK** to activate the Slot 10 card and place the Slot 8 card in standby.

Step 8 If you then see the CTNEQPT-PBWORK condition raised against all I/O cards in the node, verify that CTNEQPT-PBPROT has cleared on all I/O cards. Seeing CTNEQPT-PBWORK on the cards indicates that Slot 8 card has a bad oscillator. If this is indicated, complete the following substeps. Otherwise, go toStep 9.

- **a.** Replace the Slot 8 cross-connect card with a spare card. (Slot 8 remains standby.)
- **b.** Reseat the Slot 10 cross-connect card to activate the Slot 8 card and make Slot 10 standby.
- **c.** Verify that the CTNEQPT-PBWORK condition has cleared on all I/O cards.

Step 9 If you see CTNEQPT-PBPROT reported against all I/O cards in the node, this indicates that the Slot 10 card has a bad oscillator. If so, complete the following steps:

- **a.** Replace the Slot 10 cross-connect card with a spare card. (The Slot 8 card is now active.)
- **b.** Reseat the Slot 8 cross-connect card to make Slot 10 active.
- **c.** Verify that the CTNEQPT-PBPROT condition has cleared on all I/O cards.

1.8.17.2 Resolve the XC Oscillator Failure When Slot 10 XC Card is Active

Step 1 If the CTNEQPT-PBWORK condition is reported against all I/O cards in the node and the Slot 10 card is active, right-click the Slot 8 cross-connect card.

Step 2 Choose **Reset Card** and click **OK**. (Slot 10 remains active and Slot 8 remains standby.)

Step 3 If the CTNEQPT-PBWORK condition does not clear, reseat the Slot 8 cross-connect card.

Step 4 If the condition does not clear, replace the Slot 8 cross-connect card with an identical, spare card.

Step 5 If the condition does not clear, replace the spare card placed in Slot 8 with the original cross-connect card.

Step 6 Right-click the Slot 10 cross-connect card.

Step 7 Choose **Reset Card** and click **OK**. The Slot 8 cross-connect card becomes active and Slot 10 becomes standby.

Step 8 If you have switched the Slot 8 card to active and continue to see CTNEQPT-PBWORK reported against all I/O cards in the node, this indicates the Slot 8 card has a bad oscillator. If this is indicated, complete the following substeps. If not, go to Step 9.

a. Replace the Slot 8 cross-connect card with a spare card. (The Slot 10 card is made active.)

b. Reseat the Slot 10 cross-connect card to make Slot 8 active.

c. Verify that the CTNEQPT-PBWORK condition has cleared on all I/O cards.

Step 9 If you then see the CTNEQPT-PBPROT condition raised against all I/O cards, verify that CTNEQPT-PBWORK has cleared on the I/O cards. This indicates that Slot 10 has a bad oscillator. If so, complete the following substeps:

a. Replace the Slot 10 cross-connect card with a spare card. (Slot 10 remains standby.)

b. Reseat the Slot 8 cross-connect card to activate the Slot 10 card and make Slot 8 standby.

c. Verify that the CTNEQPT-PBPROT condition has cleared on all I/O cards.

1.9 Circuits and Timing

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

1.9.1 OC-N Circuit Transitions to Partial State

Symptom An automatic or manual transition of a circuit from one state to another state results in one of the following partial state conditions:

- OOS_PARTIAL: At least one of the OC-N connections in the circuit is in OOS state and at least one other connection in the circuit is in IS, OOS_MT, or OOS_AINS state.
- OOS_MT_PARTIAL: At least one connection in the OC-N circuit is in OOS_MT state and at least one other connection in the circuit is in IS, OOS_MT, or OOS_AINS state.
- OOS_AINS_PARTIAL: At least one connection in the OC-N circuit is in the OOS_AINS state and at least one other connection in the circuit is in IS or OOS_AINS state.

Table 1-27 describes the possible problems and the solutions.

Table 1-27 Circuit in Partial State

Possible Problem	Solution
During a manual transition, CTC cannot communicate with one of the nodes or one of the nodes is on a version of software that does not support the new state model.	Repeat the manual transition operation. If the partial state persists, determine which node in the circuit is not changing to the desired state. Complete the "View the State of OC-N Circuit Nodes" procedure on page 1-89. Log into the circuit node that did not change to the desired state and determine the version of software. If the software on the node is Software R3.3 or earlier, upgrade the software. Refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures. **Note** If the node software cannot be upgraded to R4.0, the partial state condition can be avoided by using only the circuit state supported in the earlier software version.
During an automatic transition, some path-level defects and/or alarms were detected on the circuit. One end of the circuit is not properly terminated.	Determine which node in the circuit is not changing to the desired state. Complete the "View the State of OC-N Circuit Nodes" procedure on page 1-89. Log onto the circuit node that did not change to the desired state and examine the circuit for path-level defects, improper circuit termination, or alarms. Refer to the *Cisco ONS 15454 Procedure Guide* for procedures to clear alarms and change circuit configuration settings. Resolve and clear the defects and/or alarms on the circuit node and verify that the circuit transitions to the desired state.

View the State of OC-N Circuit Nodes

Note This procedure does not apply to Software R4.6 DWDM cards.

Step 1 Click the **Circuits** tab.

Step 2 From the Circuits tab list, select the circuit with the ***_PARTIAL status condition.

Step 3 Click **Edit**. The Edit Circuit window appears.

Step 4 In the Edit Circuit window, click the **State** tab (if you are viewing a SONET circuit).

The State tab window lists the Node, CRS End A, CRS End B, and CRS State for each of the nodes in the circuit.

1.9.2 AIS-V on DS3XM-6 Unused VT Circuits

Symptom An incomplete circuit path causes an AIS.

Table 1-28 describes the possible problem and the solution.

Table 1-28 Calculate and Design IP Subnets

Possible Problem	Solution
The port on the reporting node is in-service but a node upstream on the circuit does not have an OC-N port in service.	An AIS-V indicates that an upstream failure occurred at the virtual tributary (VT) layer. AIS-V alarms also occur on DS3XM-6 VT circuits that are not carrying traffic and on stranded bandwidth. Complete the "Clear AIS-V on DS3XM-6 Unused VT Circuits" procedure on page 1-90.

Clear AIS-V on DS3XM-6 Unused VT Circuits

Note This procedure does not apply to Software R4.6 DWDM cards or ML-Series cards.

Step 1 Determine the affected port.

Step 2 Record the node ID, slot number, port number, or VT number.

Step 3 Create a unidirectional VT circuit from the affected port back to itself, such as Source node/Slot 2/Port 2/VT 13 cross connected to Source node/Slot 2/Port 2/VT 13.

Step 4 Uncheck the bidirectional check box in the circuit creation window.

Step 5 Give the unidirectional VT circuit an easily recognizable name, such as "delete me."

Step 6 Display the DS3XM-6 card in CTC card view. Click the **Maintenance** > **DS1** tabs.

Step 7 Locate the VT that is reporting the alarm (for example, DS3 #2, DS1 #13).

Step 8 From the Loopback Type list, choose **Facility (Line)** and click **Apply**.

Step 9 Click **Circuits**.

Step 10 Find the one-way circuit you created in Step 3. Select the circuit and click **Delete**.

Step 11 Click **Yes** in the Delete Confirmation dialog box.

Step 12 Display the DS3XM-6 card in CTC card view. Click **Maintenance** > **DS1**.

Step 13 Locate the VT in Facility (line) Loopback.

Step 14 From the Loopback Type list, choose **None** and then click **Apply**.

Step 15 Click the **Alarms** tab and verify that the AIS-V alarms have cleared.

Step 16 Repeat this procedure for all the AIS-V alarms on the DS3XM-6 cards.

1.9.3 Circuit Creation Error with VT1.5 Circuit

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

Table 1-29 describes the possible problem and the solution.

Table 1-29 Circuit Creation Error with VT1.5 Circuit

Possible Problem	Solution
You might have run out of bandwidth on the VT cross-connect matrix at the ONS 15454 indicated in the error message.	The matrix has a maximum capacity of 336 bidirectional VT1.5 cross-connects. Certain configurations exhaust VT capacity with less than 336 bidirectional VT1.5s in a BLSR or less than 224 bidirectional VT1.5s in a path protection or 1+1 protection group. Refer to the *Cisco ONS 15454 Reference Guide* for more information.

1.9.4 Unable to Create Circuit From DS-3 Card to DS3XM-6 Card

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

Table 1-30 describes the possible problem and the solution.

Table 1-30 Unable to Create Circuit from DS-3 Card to DS3XM-6 Card

Possible Problem	Solution
A DS-3 card and a DS3XM-6 card have different functions.	A DS3XM-6 card converts each of its six DS-3 interfaces into 28 DS-1s for cross-connection through the network. Thus, you can create a circuit from a DS3XM-6 card to a DS-1 card, but not from a DS3XM-6 card to a DS-3 card. These differences are evident in the STS path overhead. The DS-3 card uses asynchronous mapping for DS-3, which is indicated by the C2 byte in the STS path overhead that has a hex code of 04. A DS3XM-6 has a VT payload with a C2 hex value of 02. **Note** You can find instructions for creating circuits in the *Cisco ONS 15454 Procedure Guide*.

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

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

Table 1-31 on page 1-91 describes the possible problem and the solution.

Table 1-31 DS3 Card Does Not Report AIS-P From External Equipment

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

1.9.6 OC-3 and DCC Limitations

Symptom Limitations to OC-3 and DCC usage.

Table 1-32 describes the possible problem and the solution.

Table 1-32 OC-3 and DCC Limitations

Possible Problem	Solution
OC-3 and DCC have limitations for the ONS 15454.	For an explanation of OC-3 and DCC limitations, refer to the DCC Tunnels section of the *Cisco ONS 15454 Procedure Guide*.

1.9.7 ONS 15454 Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

Table 1-33 describes the possible problems and the solution.

Table 1-33 ONS 15454 Switches Timing Reference

Possible Problem	Solution
The optical or BITS input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source.	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 x 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.
The optical or building integrated timing supply (BITS) input is not functioning.	
The synchronization status messaging (SSM) message is set to do not use for synchronization (DUS).	
SSM indicates a Stratum 3 or lower clock quality.	
The input frequency is off by more than 15 ppm.	
The input clock wanders and has more than three slips in 30 seconds.	
A bad timing reference existed for at least two minutes.	

1.9.8 Holdover Synchronization Alarm

Symptom The clock is running at a different frequency than normal and the "HLDOVRSYNC" alarm appears.

Table 1-34 describes the possible problem and the solution.

Table 1-34 Holdover Synchronization Alarm

Possible Problem	Solution
The last reference input has failed.	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 "2.7.128 HLDOVRSYNC" section on page 2-104 for a detailed description of this alarm. **Note** The ONS 15454 supports holdover timing per Telcordia GR-436 when provisioned for external (BITS) timing.

1.9.9 Free-Running Synchronization Mode

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

Table 1-35 describes the possible problem and the solution.

Table 1-35 Free-Running Synchronization Mode

Possible Problem	Solution
No reliable reference input is available.	The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the "FRNGSYNC" condition on page 2-96 for a detailed description.

1.9.10 Daisy-Chained BITS Not Functioning

Symptom You are unable to daisy chain the BITS sources.

Table 1-36 describes the possible problem and the solution.

Table 1-36 Daisy-Chained BITS Sources Not Functioning

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

1.9.11 Blinking STAT LED after Installing a Card

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

Table 1-37 describes the possible problem and the solution.

Table 1-37 Blinking STAT LED on Installed Card

Possible Problem	Solution
The card cannot boot because it failed the Power On Shelf Test (POST) diagnostics.	The blinking STAT LED indicates that POST diagnostics are being performed. If the LED continues to blink more than 60 seconds, the card has failed the POST diagnostics test and has failed to boot. If the card has truly failed, an "EQPT" alarm is raised against the slot number with an "Equipment Failure" description. Check the alarm tab for this alarm to appear for the slot where the card was installed. To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card. Complete the "Physically Replace a Card" procedure on page 2-219. ⚠ **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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

1.10 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.

1.10.1 Bit Errors Appear for a Traffic Card

Symptom A traffic card has multiple bit errors.

Table 1-38 describes the possible problem and the solution.

Table 1-38 Bit Errors Appear for a Line Card

Possible Problem	Solution
Faulty cabling or low optical-line levels.	Bit errors on line (traffic) cards usually originate from cabling problems or low optical-line levels. The errors can be caused by synchronization problems, especially if PJ (pointer justification) errors are reported. Moving cards into different error-free slots will isolate the cause. Use a test set whenever possible because the cause of the errors could be external cabling, fiber, or external equipment connecting to the ONS 15454. Troubleshoot cabling problems using the "1.1 Network Troubleshooting Tests" section on page 1-2. Troubleshoot low optical levels using the "1.10.2 Faulty Fiber-Optic Connections" section on page 1-95.

1.10.2 Faulty Fiber-Optic Connections

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

Table 1-39 describes the possible problems and the solutions.

Table 1-39 Faulty Fiber-Optic Connections

Possible Problem	Solution
Faulty fiber-optic connections.	Faulty fiber-optic connections can be the source of SONET/DWDM alarms and signal errors. Complete the "Verify Fiber-Optic Connections" procedure on page 1-95.
Faulty CAT-5 cables.	Faulty CAT-5 cables can be the source of SONET/DWDM alarms and signal errors. Complete the "1.10.2.1 Crimp Replacement LAN Cables" section on page 1-97.
Faulty Gigabit Interface Converters (GBIC).	Faulty GBICs can be the source of SONET/DWDM alarms and signal errors. See the "1.10.2.2 Replace Faulty GBIC or SFP Connectors" section on page 1-98.

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

Verify Fiber-Optic Connections

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

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

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

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

- **a.** Remove the Rx end of the suspect fiber.
- **b.** Connect the receive end of the suspect fiber to a fiber-optic power meter, such as a GN Nettest LP-5000.
- **c.** Determine the power level of fiber with the fiber-optic power meter.
- **d.** Verify the power meter is set to the appropriate wavelength for the OC-N card being tested (either 1310 nm or 1550 nm depending on the specific card).
- **e.** Verify that the power level falls within the range specified for the card if it is an OC-N card; see the "1.10.3 OC-N Card Transmit and Receive Levels" section on page 1-102.

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

a. Clean or replace the fiber patch cords. Clean the fiber according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

b. Clean the optical connectors on the card. Clean the connectors according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

c. Ensure that the far-end transmitting card is not an ONS intermediate-range (IR) card when an ONS long-range (LR) card is appropriate.

IR cards transmit a lower output power than LR cards.

d. Replace the far-end transmitting OC-N card to eliminate the possibility of a degrading transmitter on this OC-N card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

e. If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):

- Excessive fiber distance; single-mode fiber attenuates at approximately 0.5 dB/km.
- Excessive number or fiber connectors; connectors take approximately 0.5 dB each.
- Excessive number of fiber splices; splices take approximately 0.5 dB each.

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

Step 5 If no power level shows on the fiber, the fiber is bad or the transmitter on the OC-N card failed.

a. Check that the Tx and Rx fibers are not reversed. LOS and EOC alarms normally accompany reversed Tx and Rx fibers. Switching reversed Tx and Rx fibers clears the alarms and restores the signal.

b. Clean or replace the fiber patch cords. Clean the fiber according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

c. Retest the fiber power level.

d. If the replacement fiber still shows no power, replace the OC-N card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

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

Receiver overloads occur when maximum receiver power is exceeded.

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

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

1.10.2.1 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 1-34 shows the wiring of an RJ-45 connector. Figure 1-35 shows a LAN cable layout, and Table 1-40 shows the cable pinouts. Figure 1-36 shows a cross-over cable layout, and Table 1-41 shows the cross-over pinouts.

Figure 1-34 RJ-45 Pin Numbers

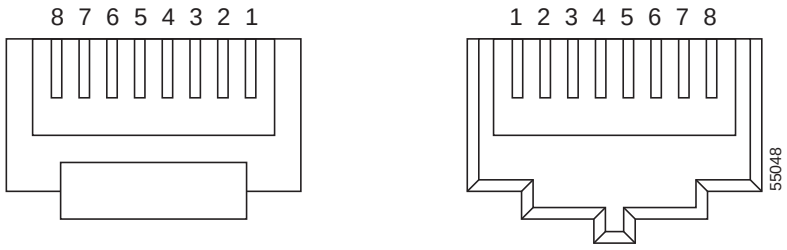


Figure 1-35 LAN Cable Layout

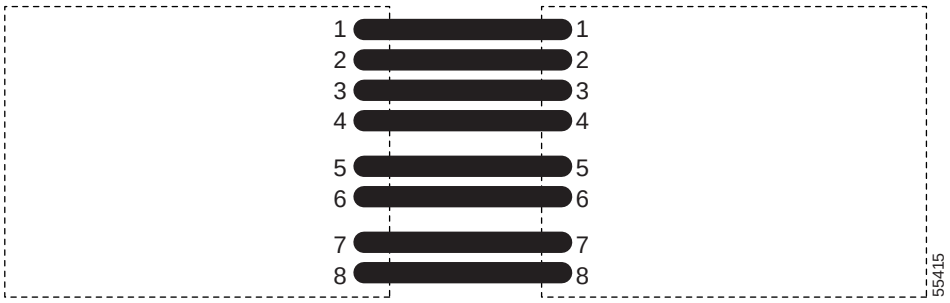


Table 1-40 LAN Cable Pinout

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 1-36 Cross-Over Cable Layout

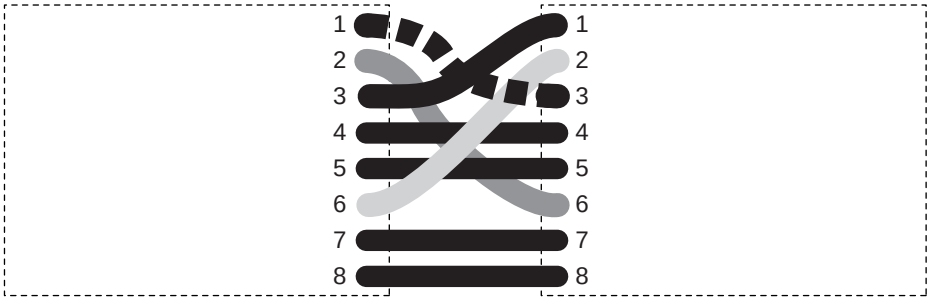


Table 1-41 Cross-Over Cable Pinout

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.

1.10.2.2 Replace Faulty GBIC or SFP Connectors

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

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

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

GBICs and SFPs are input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. The type of GBIC or SFP determines the maximum distance that the Ethernet traffic can travel from the card to the next network device. For a description of GBICs and SFPs and their capabilities, see Table 1-42 and Table 1-43 on page 1-100, and refer to the *Cisco ONS 15454 Reference Guide*.

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

Note DWDM and coarse wavelength division multiplexing (CWDM) GBICs do not function with Software R4.6.

GBICs are available in two different models. One GBIC model has two clips (one on each side of the GBIC) that secure the GBIC in the slot on the E1000-2-G, G-Series, or G1K-4 card. The other model has a locking handle. Both models are shown in Figure 1-37.

Figure 1-37 GBICs

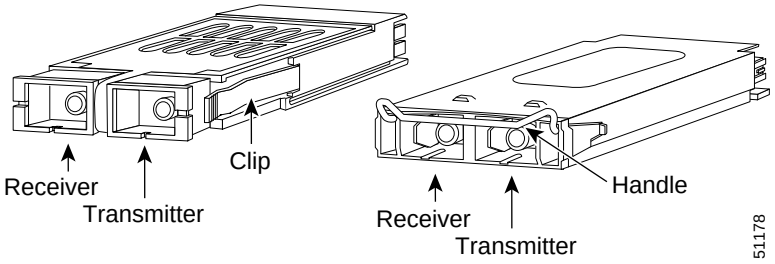


Table 1-42 shows the available GBICs. Table 1-43 shows the available SFPs.

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

Table 1-42 Available GBICs

GBIC	Associated Cards	Application	Fiber	Product Number
1000BaseSX	E1000-2-G G-Series G1K-4	Short reach	Multimode fiber up to 550 m long	15454E-GBIC-SX=

Table 1-42 Available GBICs (continued)

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

Table 1-43 Available SFPs

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

Remove GBIC or SFP Connectors

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

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

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

Step 3 Slide the GBIC or SFP out of the Gigabit Ethernet module slot. A flap closes over the GBIC or SFP slot to protect the connector on the Gigabit Ethernet card.

Installing a GBIC with Clips

Step 1 Remove the GBIC from its protective packaging.

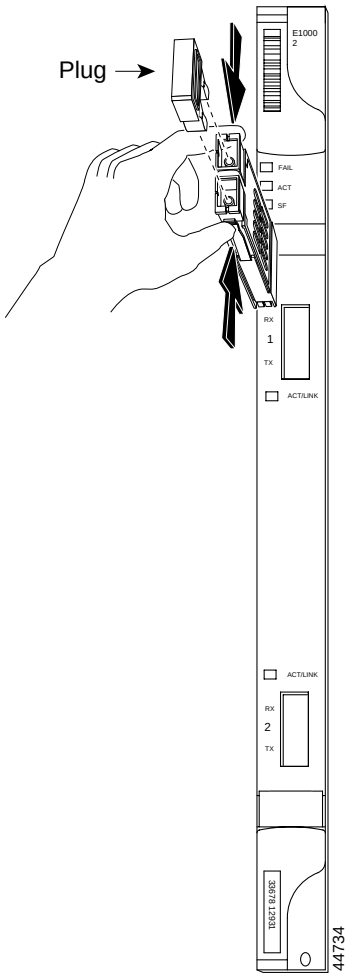
Step 2 Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.

Step 3 Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

Step 4 Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, or G-Series card (Figure 1-38).

Note GBICs are keyed to prevent incorrect installation.

Figure 1-38 GBIC Installation (with Clips)



Step 5 Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.

Step 6 When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.

Step 7 Return to your originating procedure (NTP).

Installing a GBIC with a Handle

Step 1 Remove the GBIC from its protective packaging.

Step 2 Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.

Step 3 Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

Step 4 Remove the protective plug from the SC-type connector.

Step 5 Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, G1K-4, or G-Series card.

Note GBICs are keyed to prevent incorrect installation.

Step 6 Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to SC-type connector.

Step 7 Return to your originating procedure (NTP).

1.10.3 OC-N Card Transmit and Receive Levels

Each OC-N card has a transmit and receive connector on its faceplate. Table 1-44 lists these levels.

Table 1-44 OC-N Card Transmit and Receive Levels

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

1.11 Power and LED Tests

This section provides symptoms and solutions for power supply, power consumption, and LED indicator problems.

1.11.1 Power Supply Problems

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

Table 1-45 describes the possible problems and the solution.

Table 1-45 Power Supply Problems

Possible Problem	Solution
Loss of power or low voltage.	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** tabs and change the Date and Time fields. Complete the "Isolate the Cause of Power Supply Problems" procedure on page 1-103.
Improperly connected power supply.	

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

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

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

Isolate the Cause of Power Supply Problems

Step 1 If a single ONS 15454 show signs of fluctuating power or power loss:

- **a.** Verify that the –48 VDC #8 power terminals are properly connected to a fuse panel. These power terminals are located on the lower section of the backplane EIA under the clear plastic cover.
- **b.** Verify that the power cable is #12 or #14 AWG and in good condition.
- **c.** Verify that the power cable connections are properly crimped. Stranded #12 or #14 AWG does not always crimp properly with Staycon type connectors.
- **d.** Verify that 20-A fuses are used in the fuse panel.
- **e.** Verify that the fuses are not blown.

f. Verify that a rack-ground cable attaches to the frame-ground terminal (FGND) on the right side of the ONS 15454 EIA. Connect this cable to the ground terminal according to local site practice.

g. Verify that the DC power source has enough capacity to carry the power load.

h. If the DC power source is battery-based:

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

Step 2 If multiple pieces of site equipment show signs of fluctuating power or power loss:

a. Check the uninterruptible power supply (UPS) or rectifiers that supply the equipment. Refer to the UPS manufacturer's documentation for specific instructions.

b. Check for excessive power drains caused by other equipment, such as generators.

c. Check for excessive power demand on backup power systems or batteries when alternate power sources are used.

1.11.2 Power Consumption for Node and Cards

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

Table 1-46 describes the possible problem and the solution.

Table 1-46 Power Consumption for Node and Cards

Possible Problem	Solution
Improper power supply.	Refer to power information in the *Cisco ONS 15454 Reference Guide*.

1.11.3 Lamp Tests for Card LEDs

The LED lamp test determines whether card-level LEDs are operational. For optical and electrical cards, this test also causes port-level LEDs to illuminate. For all other data cards, only card-level LEDs light. For these cards, port-level LEDs can be compared to the given guidelines to determine whether they are working correctly.

Symptom Optical (OC-N) or electrical (DS-N) card LEDs do not light, or you are unsure whether the LEDs are working properly.

Optical and electrical port LEDs light during the lamp test. Other data card types only illuminate card-level LEDs during the test. Table 1-47 describes the possible problem and the solution for optical and electrical cards.

Table 1-47 Lamp Test for Optical and Electrical Card LEDs

Possible Problem	Solution
Faulty optical and electrical port LED	A lamp test verifies that all the port LEDs work. Run this diagnostic test as part of the initial ONS 15454 turn-up, a periodic maintenance routine, or any time you question whether an LED is in working order. Complete the "Verify Card LED Operation" procedure on page 1-105.

Verify Card LED Operation

Step 1 In CTC, click the **Maintenance** > **Diagnostic** tabs.

Step 2 Click **Lamp Test**.

Step 3 Watch to make sure all the port LEDs illuminate as previously noted for several seconds.

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

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

Symptom G-Series Ethernet or FC_MR-4 card LED does not light, or you are unsure if LEDs are working properly.

Table 1-48 describes the possible problem and the solution for G-Series and FC_MR-4 cards.

Note G-Series and FC_MR-4 card-level LEDs illuminate during a lamp test, but the port-level LEDs do not.

Table 1-48 Lamp Test for G-Series or FC_MR-4 Card LEDs

Possible Problem	Solution
Faulty LED	Complete the "Verify G-Series Ethernet or FC_MR-4 Card LED Operation" procedure on page 1-105.

Verify G-Series Ethernet or FC_MR-4 Card LED Operation

Step 1 Complete the "Verify Card LED Operation" procedure on page 1-105 to verify that card-level LEDs are operational.

Step 2 Use the following list of guidelines to physically test whether the G-Series Ethernet port LEDs are operating correctly. If the LED appears as described when the listed state is occurring for the port, the LED is considered to be functioning correctly.

- Clear port LED: Should only occur if there is a loss of receive link (such as a disconnected link or unplugged GBIC). An LOS alarm could be present on the port.
- Amber port LED: Should only occur if a port is disabled but the link is connected; or if the port is enabled and the link is connected, but a transport failure is present. A TPTFAIL alarm can be present on the port.

- Green port LED: Should occur if the port is enabled and has no errors against it or traffic in it; can also occur if the port is enabled, has no errors, and is running traffic proportionate to the blink rate. No traffic-affecting port alarms should be present.

Step 3 If you are unable to determine the port state, contact Cisco TAC (1 800 553-2447).

Symptom E-Series or ML-Series Ethernet card LED does not light, or you are unsure if LEDs are working properly.

Table 1-48 describes the possible problem and the solution for E-Series and ML-Series Ethernet cards.

Note E-Series and ML-Series card-level LEDs illuminate during a lamp test, but the port-level LEDs do not.

Table 1-49 Lamp Test for E-Series and ML-Series Ethernet Card LEDs

Possible Problem	Solution
Faulty LED	Complete the "Verify E-Series and ML-Series Ethernet Card LED Operation" procedure on page 1-106.

Verify E-Series and ML-Series Ethernet Card LED Operation

Step 1 Complete the "Verify Card LED Operation" procedure on page 1-105 to verify that card-level LEDs are operational.

Step 2 Use the following list of guidelines to physically test whether the single E-Series or ML-Series Ethernet port LED is operating correctly. If the LED appears as described when the listed state is occurring for the port, the LED is considered to be functioning correctly.

- Clear port LED: Should only occur is there is a loss of receive link (such as a disconnected link or unplugged GBIC), or if traffic is flowing in one direction (either transmit or receive). A CARLOSS alarm could be present on the port.
- Amber port LED: Should only occur if the link is connected and the physical port is transmitting and receiving traffic.
- Green port LED: Should occur if the link is up and no traffic is flowing on the port.

Step 3 If you are unable to determine the port state, contact Cisco TAC (1 800 553-2447).