General Troubleshooting

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

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15327. To troubleshoot specific ONS 15327 alarms, see Chapter 2, "Alarm Troubleshooting." If you cannot find what you are looking for contact the Cisco Technical Assistance Center (Cisco TAC).

This chapter includes the following sections on network problems:

- 1.1 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 15327 Procedure Guide*.

- 1.2 Identify Points of Failure on a DS-N Circuit Path—Describes the steps to perform loopback and hairpin tests, which you can use to test DS-N circuit paths through the network or logically isolate faults.
- 1.3 Identify Points of Failure on an OC-N Circuit Path—Describes the steps to perform loopback and hairpin tests, which you can use to test OC-N circuit paths through the network or logically isolate faults.

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

- 1.4 Restoring the Database and Default Settings—Provides procedures for restoring software data and restoring the node to the default setup.
- 1.5 PC Connectivity Troubleshooting—Provides troubleshooting procedures for PC and network connectivity to the ONS 15327.
- 1.6 CTC Operation Troubleshooting—Provides troubleshooting procedures for CTC login or operation problems.
- 1.7 Circuits and Timing—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.

- 1.8 Fiber and Cabling—Provides troubleshooting procedures for fiber and cabling connectivity errors.

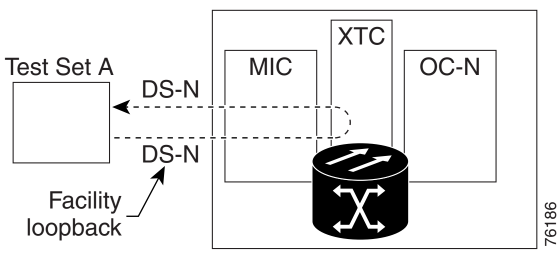
1.1 Network Troubleshooting Tests

Use loopbacks and hairpins to test newly created circuits before running live traffic or to logically locate the source of a network failure. All ONS 15327 line (traffic) cards, except E-Series Ethernet cards, allow loopbacks and hairpins.

Caution On OC-N cards, a facility 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 loopback tests the line interface unit (LIU) of a card, the mechanical interface card (MIC), 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 MIC, or the cabling plant as the potential cause of a network problem. Figure 1-1 shows a facility loopback on an XTC-14 or XTC-28-3 card.

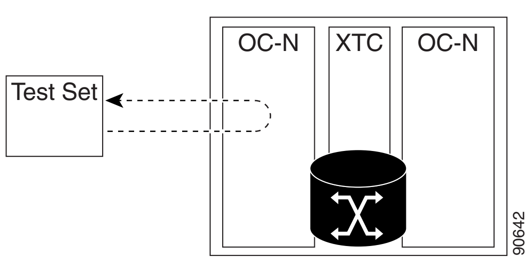
Figure 1-1 Facility Loopback Process on an XTC Card



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

Caution Before performing a facility loopback on an OC-N card, make 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, thus enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the ONS 15327 containing the loopback OC-N card.

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



A terminal loopback tests a circuit path as it passes through the XTC card and loops back from the card with the loopback. Figure 1-3 on page 1-3 shows a terminal loopback on an OC-N card. The test-set traffic comes in on the MIC card DS-N ports and goes through the XTC 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 XTC card to the MIC card. This test verifies that the XTC card cross-connect circuit paths are valid, but does not test the LIU on the OC-N card.

Setting a terminal loopback on the G-Series card may 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 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 may also continue to increment when the G-Series card is in terminal loopback. 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

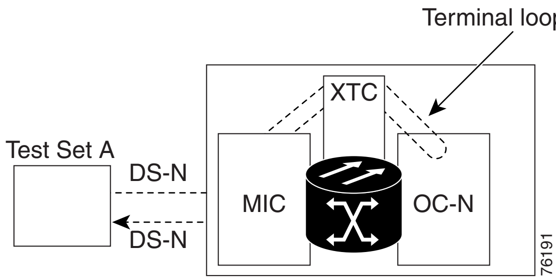
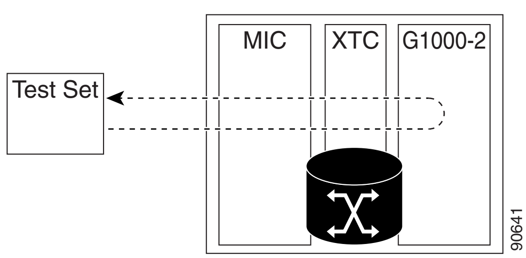


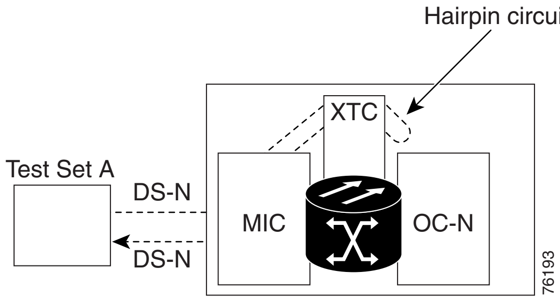
Figure 1-4 shows a terminal loopback on a G1000-2 card. The test-set traffic comes in on the MIC card DS-N ports and goes through the XTC card to the G1000-2 card. The terminal loopback on the G1000-2 card turns the signal around before it reaches the LIU and sends it back through the XTC card to the MIC card. This test verifies that the XTC card cross-connect circuit paths are valid, but does not test the LIU on the G1000-2 card.

Figure 1-4 Terminal Loopback Process on a G1000-2 Card



A hairpin circuit brings traffic in and out on a DS-N port instead of sending the traffic onto the OC-N. A hairpin loops back only the specific STS or VT circuit and does not cause an entire OC-N port to loop back, which would drop all traffic on the OC-N port. The hairpin allows you to test a circuit on nodes running live traffic. Figure 1-5 shows the hairpin circuit process on a OC-N card.

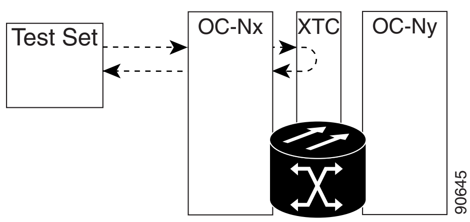
Figure 1-5 Hairpin Circuit Process on an OC-N Card



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 without interrupting the other STS circuits.

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. Figure 1-6 shows a cross-connect loopback on an OC-N port.

Figure 1-6 Cross-Connect Loopback Process on an OC-N Port



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

Facility loopbacks, hairpin circuits, and terminal loopbacks 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 an DS-N circuit on a two-node bidirectional line switched ring (BLSR). Using a series of facility loopbacks, hairpin circuits, and terminal loopbacks, the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of network test procedures applies to this scenario:

1. Facility loopback on the source-node XTC port
2. Hairpin on the source-node XTC port
3. Terminal loopback to the destination-node XTC port
4. Hairpin on the destination-node XTC port
5. Facility loopback to the destination XTC port

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

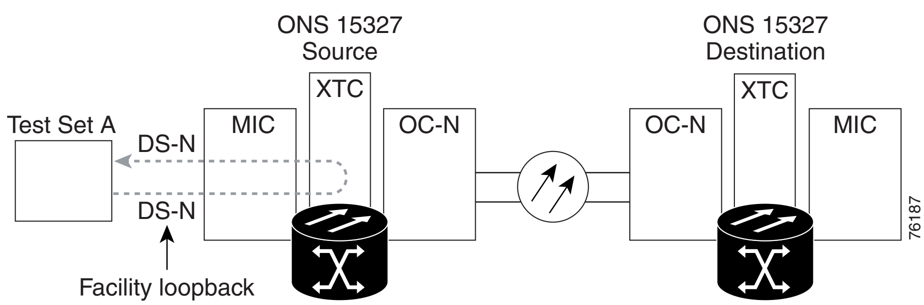
Note All loopback tests require on-site personnel.

Note These procedures are performed when power connections to the node(s) or site(s) are assumed to be within necessary specifications. If the network tests do not isolate the problems, troubleshoot outward for power failure.

1.2.1 Perform a Facility Loopback on a Source XTC Port

The facility loopback test is performed on the node source port in the network circuit; in this example, the test is routed through the MIC card and performed on the XTC port in the source node. Completing a successful facility loopback on this port isolates the cabling, MIC card, and XTC card as possible failure points. Figure 1-7 shows an example of a facility loopback on a source node XTC port.

Figure 1-7 Facility Loopback on a Source XTC Port



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

Note Loopbacks operate only on ports in the out of service-maintenance (OOS_MT) state.

Procedure: Create the Facility Loopback on the Source XTC Port

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

Use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the MIC card, which interfaces with the XTC card. Both Tx and Rx connect to the same port. Adjust the test set accordingly.

Step 2 Use CTC to create the facility loopback on the port being tested:

a. In node view, double-click the card where you are performing the loopback.

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

c. 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.

d. 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.

e. Click the **Apply** button.

f. Click the **Yes** button in the Confirmation Dialog box.

Note It is normal for a LPBKFACILITY condition to appear during loopback setup. The condition clears when you remove the loopback.

Step 3 Proceed to the "Test the Facility Loopback" procedure on page 1-6.

Procedure: Test the Facility Loopback

Step 1 If the test set is not already sending traffic, send test-set 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:

a. Clear the loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

b. Proceed to the "Perform a Cross-Connect Loopback on the Source OC-N Port" procedure on page 1-24.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty MIC card, faulty XTC card, or faulty cabling from the DS-N port.

Step 5 Proceed to the "Test the DS-N Cabling" procedure on page 1-6.

Procedure: Test the DS-N Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the MIC ports) with a cable known to be good.

If a cable known to be good is not available, test the suspect cable with a test set. Remove the suspect cable from the MIC and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or suspect.

Step 2 Resend test-set traffic on the loopback circuit with a good cable installed.

Step 3 If the test set indicates a good circuit, the problem is probably the defective cable:

a. Replace the defective cable.

b. Clear the loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

c. Proceed to the "Perform a Cross-Connect Loopback on the Source OC-N Port" procedure on page 1-24.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Proceed to the "Test the XTC Card" procedure on page 1-7.

Procedure: Test the XTC Card

Step 1 Replace the suspect card with a card known to be good.

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

Step 3 If the test set indicates a good circuit, the problem is probably a defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the faulty card.

c. Clear the loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

d. Proceed to the "Perform a Hairpin on a Source Node XTC Port" procedure on page 1-9.

Step 4 If the test set indicates a fault circuit, the problem might be faulty cabling from the MIC card to the XTC card or a faulty MIC card.

Step 5 Proceed to the "Test the MIC Cabling" procedure on page 1-8.

Procedure: Test the MIC Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the MIC or from the MIC to the XTC) with a cable that is known to be good.

If a good cable is not available, test the suspect cable with a test set. Remove the suspect cable 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 cable that is known to be good installed.

Step 3 If the test set indicates a good circuit, the problem is probably the defective cable:

a. Replace the defective cable.

b. Clear the facility loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

c. Proceed to the "Perform a Hairpin on a Source Node XTC Port" procedure on page 1-9.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty MIC card.

Step 5 Proceed to the "Test the MIC Card" procedure on page 1-8.

Procedure: Test the MIC Card

Step 1 Replace the suspect card with a good card. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably a defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

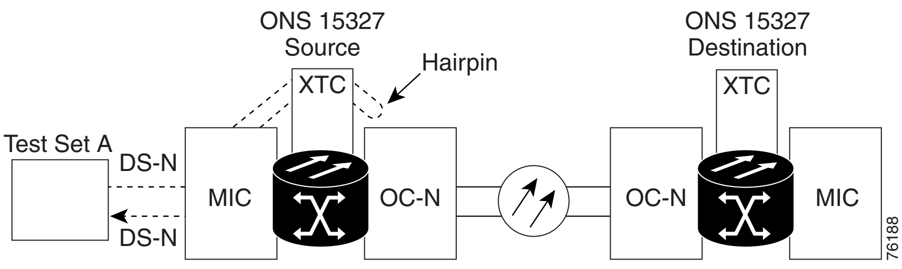
Step 4 If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

Step 5 Proceed to the "1.2.2 Perform a Hairpin on a Source Node XTC Port" section on page 1-9.

1.2.2 Perform a Hairpin on a Source Node XTC Port

The hairpin test is performed on the first XTC card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through this card isolates the possibility that the source XTC card is the cause of the faulty circuit. Figure 1-8 on page 1-9 shows an example of a hairpin circuit on a source node XTC port.

Figure 1-8 Hairpin Circuit on a Source Node XTC Port



Note An XTC card is required to operate the ONS 15327 and can be used in a redundant or nonredundant configuration.

Procedure: Create the Hairpin on the Source Node Port

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

- If you just completed the "Perform a Facility Loopback on a Source XTC Port" procedure on page 1-5, leave the electrical test set hooked up to the MIC port.
- If you are starting the current procedure without the electrical test set hooked up to the MIC port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the MIC connectors for the port you are testing. The Tx and Rx terminals connect to the same port.

Adjust the test set accordingly.

Step 2 Use CTC to set up the hairpin on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as Hairpin1.

c. Set the circuit **Type** and **Size** to the normal preferences.

d. Uncheck the **Bidirectional** check box and click the **Next** button.

e. In the Circuit Source dialog box, select the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.

f. In the Circuit Destination dialog box, use the same **Node**, card **Slot**, **Port**, and **Type** used for the Circuit Source dialog box and click the **Finish** button.

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

Step 4 Proceed to the "Test the Hairpin Circuit" procedure on page 1-10.

Procedure: Test the Hairpin Circuit

Step 1 If the test set is not already sending traffic, send test-set 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 loopback circuit:

a. Clear the hairpin circuit:

- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.
- Confirm that the hairpin circuit is deleted from the Circuits tab list.

b. Proceed to the "Perform a Terminal Loopback on a Destination XTC Port" procedure on page 1-12.

Step 4 If the test set indicates a faulty circuit, there might be a problem with the XTC card.

Step 5 Proceed to the "Test the Alternate Source XTC Card" procedure on page 1-10.

Procedure: Test the Alternate Source XTC Card

Step 1 Perform a reset on the active XTC card:

a. Determine the active XTC card. On both the physical node and the Cisco Transport Controller (CTC) window, the active XTC card has a green ACT LED, and the standby XTC card has an amber SBY LED.

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

c. Right-click and choose **Reset** from the shortcut menu.

d. On the Resetting Card dialog box, click **Yes**. After 20 to 40 seconds, a "lost node connection, changing to network view" message is displayed.

e. Click **OK**. On the network view map, the node where you reset the XTC is gray.

f. After the node icon turns green (within 1 to 2 minutes), double-click it. On the shelf graphic, observe the following:

- The previous standby XTC displays a green ACT LED.
- The previous active XTC LEDs go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (XTC is in standby mode).
- The LEDs should complete this sequence within 5 to 10 minutes.

Step 2 Resend test traffic on the loopback circuit. The test-set traffic now travels through the alternate XTC card.

Step 3 If the test set indicates a faulty circuit, assume that the XTC card is not causing the problem:

a. Clear the hairpin circuit:
   - Click the **Circuits** tab.
   - Choose the hairpin circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.
   - Confirm that the hairpin circuit is deleted from the Circuits tab list.

b. Proceed to the "Perform a Terminal Loopback on a Destination XTC Port" procedure on page 1-12.

Step 4 If the test set indicates a good circuit, the problem might be a defective card.

Step 5 To confirm a defective original XTC card, proceed to the "Retest the Original Source XTC Card" procedure on page 1-11.

Procedure: Retest the Original Source XTC Card

Step 1 Perform a side switch of the XTC cards to make the original card the active card.

Step 2 Resend test-set traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit on the original card, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the defective XTC card. See Chapter 3, "Replace Hardware" for details.

c. Clear the hairpin circuit:
   - Click the **Circuits** tab.
   - Choose the hairpin circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.
   - Confirm that the hairpin circuit is deleted from the Circuits tab list.

d. Proceed to Step 5.

Step 4 If the test set indicates a good circuit, the original XTC card might have had a temporary problem that is cleared by the side switch.

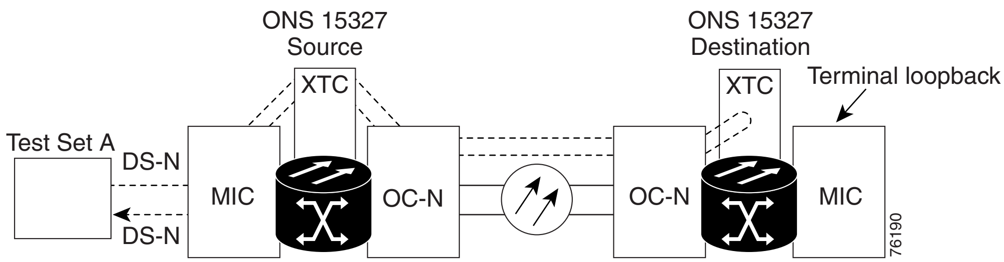
Clear the hairpin circuit:
   - Click the **Circuits** tab.
   - Choose the hairpin circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.
   - Confirm that the hairpin circuit is deleted from the Circuits tab list.

Step 5 Proceed to the "1.2.3 Perform a Terminal Loopback on a Destination XTC Port" section on page 1-12.

1.2.3 Perform a Terminal Loopback on a Destination XTC Port

The terminal loopback test is performed on the node destination port in the circuit; in this example, the XTC port in the destination node. First, create a bidirectional circuit that starts on the source node DS-N port and terminates on the destination node DS-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a destination node XTC port verifies that the circuit is good up to the destination XTC. Figure 1-9 on page 1-12 shows an example of a terminal loopback on a destination node XTC port.

Figure 1-9 Terminal Loopback on a Destination XTC Port



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

Procedure: Create the Terminal Loopback on a Destination XTC Port

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

a. If you just completed the "Perform a Hairpin on a Source Node XTC Port" procedure on page 1-9, 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 MIC card, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the MIC connectors for the port you are testing. The Tx and Rx connect to the same port.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal loopback circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as DSNtoDSN.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

e. In the Circuit Source dialog box, fill in the source **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the DS-N port in the destination node) and click the **Finish** button.

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

> **Note** Loopbacks operate only on ports in the OOS_MT state.

> **Note** It is normal for a LPBKTERMINAL condition 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 the **OK** button.

b. In node view, double-click the card that requires the loopback, such as the DS-N card in the destination node.

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 the **Apply** button.

g. Click the **Yes** button in the Confirmation Dialog box.

Step 5 Proceed to the "Test the Terminal Loopback Circuit on the Destination XTC Port" procedure on page 1-13.

Procedure: Test the Terminal Loopback Circuit on the Destination XTC Port

Step 1 If the test set is not already sending traffic, send test-set 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:

a. Clear the terminal loopback:
   - Double-click the DS-N card in the destination node with the terminal loopback.
   - Click the **Maintenance > Loopback** tabs.
   - Select **None** from the Loopback Type column for the port being tested.
   - Select the appropriate state (IS, OOS, or OOS_AINS) in the State column for the port being tested.
   - Click the **Apply** button.
   - Click the **Yes** button in the Confirmation Dialog box.

b. Clear the terminal loopback circuit:
   - Click the **Circuits** tab.
   - Choose the loopback circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.

c. Proceed to the "Perform a Hairpin on a Destination Node XTC Port" procedure on page 1-15.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Proceed to the "Test the Destination XTC Card" procedure on page 1-14.

Procedure: Test the Destination XTC Card

Step 1 Replace the suspect card with a good card. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the defective XTC card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the terminal loopback:
   - Double-click the DS-N card in the destination node with the terminal loopback.
   - Click the **Maintenance > Loopback** tabs.
   - Select **None** from the Loopback Type column for the port being tested.
   - Select the appropriate state (IS, OOS, or OOS_AINS) in the State column for the port being tested.
   - Click the **Apply** button.
   - Click the **Yes** button in the Confirmation Dialog box.

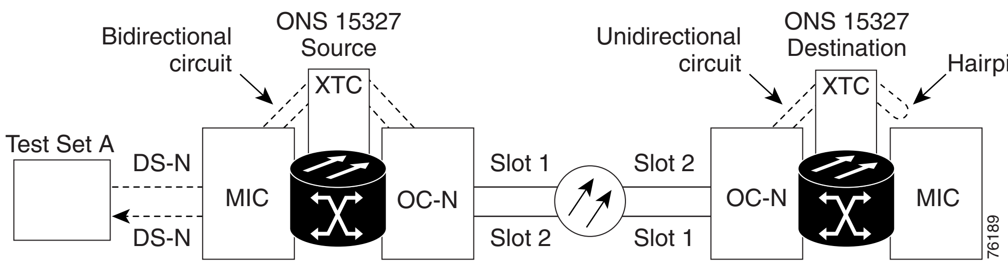
d. Clear the terminal loopback circuit:
   - Click the **Circuits** tab.
   - Choose the loopback circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.

Step 4 Proceed to the "1.2.4 Perform a Hairpin on a Destination Node XTC Port" section on page 1-15.

1.2.4 Perform a Hairpin on a Destination Node XTC Port

The hairpin test is preformed on the XTC card in the destination node. To perform this test, you must also create a bidirectional circuit from the source MIC card to the source OC-N node in the transmit direction. Creating the bidirectional circuit and completing a successful hairpin isolates the possibility that the source and destination OC-N cards, the source and destination XTC cards, or the fiber span is responsible for the faulty circuit. Figure 1-10 on page 1-15 shows an example of a hairpin circuit on a destination node XTC card.

Figure 1-10 Hairpin on a Destination Node XTC Card



Procedure: Create the Hairpin Loopback Circuit on the Destination Node XTC Card

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 Use CTC to set up the source loopback circuit on the port being tested:

- **a.** Click the **Circuits** tab and click the **Create** button.
- **b.** Give the circuit an easily identifiable name, such as Hairpin1.
- **c.** Set the circuit **Type** and **Size** to the normal preferences.
- **d.** Leave the **Bidirectional** check box checked and click the **Next** button.
- **e.** In the Circuit Source dialog box, fill in the source **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.
- **f.** In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the port in the destination node) and click the **Finish** button.

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

Step 4 Use CTC to set up the destination hairpin circuit on the port being tested.

Note The destination loopback circuit on a port is a one-way test.

For example, in a typical east-to-west slot configuration, a Slot 1 (east) OC-N card on the source node is one end of the fiber span, and the Slot 2 (west) OC-N card on the destination node is the other end.

- **a.** Click the **Circuits** tab and click the **Create** button.
- **b.** Give the circuit an easily identifiable name, such as Hairpin1.

c. Set the Circuit **Type** and **Size** to the normal preferences.

d. Uncheck the **Bidirectional** check box and click the **Next** button.

e. In the Circuit Source dialog box, select the same **Node**, card **Slot**, **Port**, and **Type** where the previous circuit is connected and click the **Next** button.

f. In the Circuit Destination dialog box, use the same **Node**, card **Slot**, **Port**, and **Type** used for the Circuit Source dialog box and click the **Finish** button.

Step 5 Confirm that the newly created circuit appears on the Circuits tab list as a one-way circuit.

Step 6 Verify that the circuits connect to the correct slots. For example, verify that source node/Slot 1 OC-N card (east slot) is connected to destination node/Slot 2(west slot). If two east slots or two west slots are connected, the circuit does not work. Except for the distinct slots, all other circuit information, such as ports, should be identical.

Step 7 Proceed to the "Test the Hairpin Circuit" procedure on page 1-16.

Procedure: Test the Hairpin Circuit

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

Step 2 Examine the test traffic received by the test set. Look for errors or any other signal information indicated by the test set.

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

a. Clear the hairpin circuit:

- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.
- Confirm that the hairpin circuit is deleted from the Circuits tab list.

b. Proceed to the "Perform a Facility Loopback on a Destination XTC Card" procedure on page 1-18.

Step 4 If the test set indicates a faulty circuit, the problem might exist with the destination XTC card.

Step 5 Proceed to the "Test the Alternate Destination XTC Card" procedure on page 1-16.

Procedure: Test the Alternate Destination XTC Card

Step 1 Perform a software reset on the active XTC card.

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

> **Note** After the active XTC goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

Step 2 Resend test traffic on the loopback circuit. The test traffic routes through the alternate XTC card.

Step 3 If the test set indicates a faulty circuit, assume that the XTC card is not causing the problem:

a. Clear the hairpin circuit:
   - Click the **Circuits** tab.
   - Choose the hairpin circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.
   - Confirm that the hairpin circuit is deleted from the Circuits tab list.

b. Proceed to the "Perform a Facility Loopback on a Destination XTC Card" procedure on page 1-18.

Step 4 If the test set indicates a good circuit, the problem might be a defective card.

Step 5 To confirm a defective original XTC card, proceed to the "Retest the Original Destination XTC Card" procedure on page 1-17.

Procedure: Retest the Original Destination XTC Card

Step 1 Perform a side switch of the XTC cards to make the original card the active card.

> **Note** After the active XTC goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

Step 2 Resend test traffic on the loopback circuit. The test traffic routes through the original XTC card.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the defective cross-connect card. See "Physically Replace a Card" procedure on page 2-130.

c. Clear the hairpin circuit:
   - Click the **Circuits** tab.
   - Choose the hairpin circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.

d. Proceed to Step 5.

Step 4 If the test set indicates a good circuit, the XTC card might have had a temporary problem that is cleared by the side switch.

Clear the hairpin circuit:

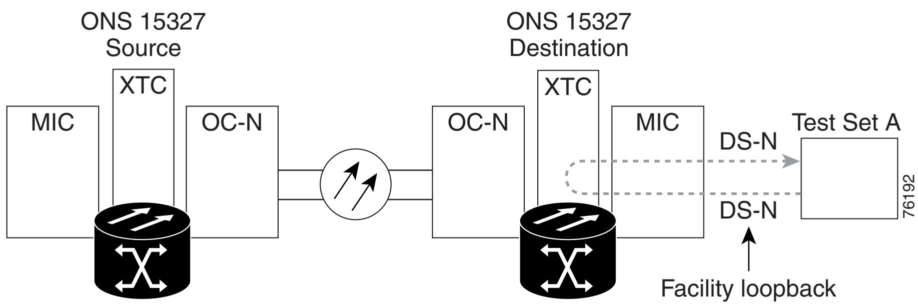
- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 5 Proceed to the "1.2.5 Perform a Facility Loopback on a Destination XTC Card" section on page 1-18.

1.2.5 Perform a Facility Loopback on a Destination XTC Card

The facility loopback test is performed on the last port in the circuit, in this case the XTC port in the destination node. Completing a successful facility loopback on this port isolates the possibility that the destination node cabling, MIC card, or line interface is responsible for a faulty circuit. Figure 1-11 shows an example of a facility loopback on a destination node XTC port.

Figure 1-11 Facility Loopback on a Destination XTC Card



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

Note Loopbacks operate only on ports in the OOS_MT state.

Procedure: Create a Facility Loopback Circuit on a Destination XTC Port

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

a. If you just completed the "Perform a Hairpin on a Destination Node XTC Port" procedure on page 1-15, 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. Both Tx and Rx connect to the same port.

c. Adjust the test set accordingly.

Step 2 Use CTC to create the facility loopback on the port being tested:

a. In node view, double-click the card where you are performing the loopback.

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

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

d. Click the **Apply** button.

e. Click the **Yes** button in the Confirmation Dialog box.

Note It is normal for a LPBKFACILITY condition to appear during loopback setup. The condition clears when you remove the loopback.

Step 3 Proceed to the "Test the Facility Loopback Circuit" procedure on page 1-19.

Procedure: Test the Facility Loopback Circuit

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

a. Clear the facility loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

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

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty MIC card or faulty cabling from the MIC card to the XTC card.

Step 5 Proceed to the "Test the DS-N Cabling" procedure on page 1-6.

Procedure: Test the DS-N Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the MIC ports) with a good cable.

If a good cable is not available, test the suspect cable with a test set. Remove the suspect cable from the MIC and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or suspect.

Step 2 Resend test traffic on the loopback circuit with a good cable installed.

Step 3 If the test set indicates a good circuit, the problem is probably the defective cable:

a. Replace the defective cable.

b. Clear the facility loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

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

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Proceed to the "Test the XTC Card" procedure on page 1-20.

Procedure: Test the XTC Card

Step 1 Replace the suspect card with a card known to be good.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the facility loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

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

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty MIC card.

Step 5 Proceed to the "Test the MIC Card" procedure on page 1-21.

Procedure: Test the MIC Card

Step 1 Replace the suspect card with a card known to be good.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (Cisco TAC).

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the facility loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

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

Step 4 If the test set indicates a faulty circuit, contact the Cisco TAC.

1.3 Identify Points of Failure on an OC-N Circuit Path

Facility loopbacks, terminal 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.

The example in this section tests an OC-N circuit on a three-node BLSR. Using a series of facility loopbacks and terminal loopbacks, the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of seven network test procedures applies to this sample scenario:

1. Facility loopback on the source-node OC-N port
2. Cross-connect loopback on the source-node OC-N port
3. Terminal loopback on the source-node OC-N port
4. Facility loopback on the intermediate-node OC-N port
5. Terminal loopback on the intermediate-node OC-N port
6. Facility loopback on the destination-node OC-N port
7. Terminal loopback on the destination-node OC-N port

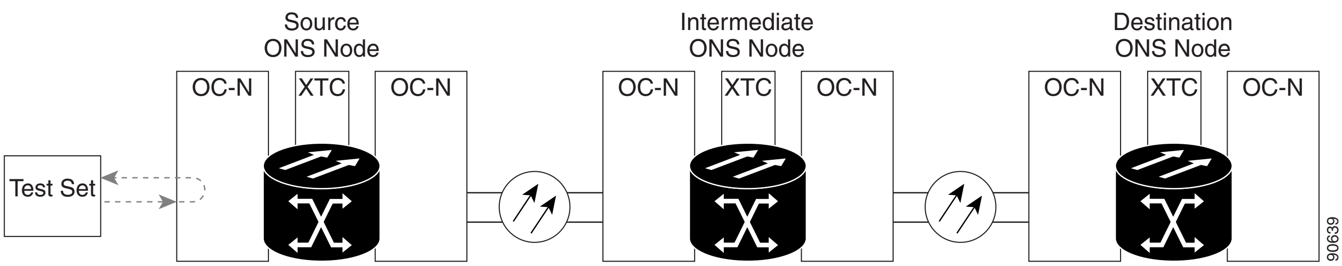
Note The test sequence for your circuits differs according to the type of circuit and network topology.

Note All loopback tests require on-site personnel.

1.3.1 Perform a Facility Loopback on a Source-Node OC-N Port

The facility loopback test is performed on the node source port in the network circuit, in this example, the source OC-N port in the source node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point. Figure 1-12 on page 1-22 shows an example of a facility loopback on a circuit source OC-N port.

Figure 1-12 Facility Loopback on a Circuit Source OC-N Port



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

Procedure: Create the Facility Loopback on the Source OC-N Port

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

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 Use CTC to create the facility loopback circuit on the port being tested:

a. In node view, double-click the card where you are performing the loopback.

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

c. 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.

d. 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.

e. Click the **Apply** button.

f. Click the **Yes** button in the Confirmation Dialog box.

Note It is normal for a LPBKFACILITY condition to appear during loopback setup. The condition clears when you remove the loopback.

Step 3 Proceed to the "Test the Facility Loopback Circuit" procedure on page 1-23.

Procedure: Test the Facility Loopback Circuit

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

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

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

a. Clear the facility loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

b. Proceed to the "Perform a Cross-Connect Loopback on the Source OC-N Port" procedure on page 1-24.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty OC-N card.

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-23.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the facility loopback:

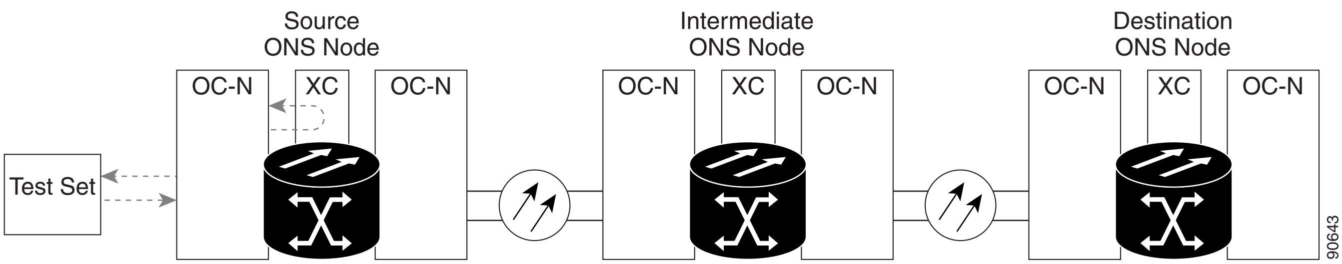
- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

Step 4 Proceed to the "1.3.2 Perform a Cross-Connect Loopback on the Source OC-N Port" section on page 1-24.

1.3.2 Perform a Cross-Connect Loopback on the Source OC-N Port

The cross-connect loopback test occurs on the cross-connect card (XCT) in a network circuit. A cross-connect loopback circuit uses the same port for both source and destination. Completing a successful cross-connect loopback through the XCT card isolates the possibility that the XCT card is the cause of the faulty circuit. Figure 1-13 on page 1-24 shows an example of a cross-connect loopback on a source OC-N port.

Figure 1-13 Cross-Connect Loopback on a Source OC-N Port



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

- **a.** If you just completed the "1.3.1 Perform a Facility Loopback on a Source-Node OC-N Port" section on page 1-22, leave the optical test set hooked up to the OC-N port in the source node.
- **b.** If you are starting the current procedure without the optical test set hooked up to the OC-N 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 put the circuit being tested out of service:

- **a.** In node view, double-click the card where the test set is connected. The card view appears.
- **b.** In card view, click the **Provisioning > Line** tabs.
- **c.** Choose **OOS** or **OOS_MT** from the Status column for the port being tested.
- **d.** Click **Apply**.
- **e.** Click **Yes** in the confirmation dialog box.

Step 3 Use CTC to set up the cross-connect loopback on the circuit being tested:

- **a.** In card view, click the **Provisioning > SONET STS** tabs.
- **b.** Click the check box in the XC Loopback column for the port being tested.
- **c.** Click **Apply**.
- **d.** Click **Yes** in the confirmation dialog box.

Step 4 Proceed to the "Test the Cross-Connect Loopback Circuit" procedure on page 1-25.

Procedure: Test the Cross-Connect Loopback Circuit

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

Step 2 Examine the test traffic 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:

a. Clear the cross-connect loopback:
   - In card view, click the **Provisioning > SONET STS** tabs.
   - Uncheck the check box in the XC Loopback column for the circuit being tested.
   - Click **Apply**.
   - Click **Yes** in the confirmation dialog.

b. Proceed to the "Perform a Terminal Loopback on a Source-Node OC-N Port" procedure on page 1-27.

Step 4 If the test set indicates a faulty circuit, there might be a problem with the cross-connect card.

Step 5 Proceed to the "Test the Standby XTC Card" procedure on page 1-25.

Procedure: Test the Standby XTC Card

Step 1 Perform a reset on the active XTC card:

a. Determine which cross-connect card is active. On both the physical node and the CTC window, the active XTC has a green ACT LED, and the standby XTC has an amber SBY LED.

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

c. Right-click and choose **Reset** from the shortcut menu.

d. On the Resetting Card dialog box, click **Yes**. After 20 to 40 seconds, a "lost node connection, changing to network view" message is displayed.

e. Click **OK**. On the network view map, the node where you reset the XTC is gray.

f. After the node icon turns green (within 1 to 2 minutes), double-click it. On the shelf graphic, observe the following:
   - The previous standby XTC displays a green ACT LED.
   - The previous active XTC LEDs go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (XTC is in standby mode).
   - The LEDs should complete this sequence within 5 to 10 minutes.

Step 2 Resend test traffic on the loopback circuit.

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

Step 3 If the test set indicates a faulty circuit, assume that the cross-connect card is not causing the problem:

a. Clear the cross-connect loopback circuit:
   - Click the **Circuits** tab.
   - Choose the cross-connect loopback circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.
   - Confirm that the cross-connect loopback circuit is deleted from the Circuits tab list.

b. Proceed to "Perform a Terminal Loopback on a Source-Node OC-N Port" procedure on page 1-27.

Step 4 If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 5 Proceed to the "Retest the Original XTC Card" procedure on page 1-26.

Procedure: Retest the Original XTC Card

Step 1 Do a manual switch of the XTC cards to make the original XTC card the active card:

a. Determine the active cross-connect card. On both the physical node and the CTC window, the active XTC has a green ACT LED, and the standby XTC has an amber SBY LED.

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

c. Right-click and choose **Reset** from the shortcut menu.

d. On the Resetting Card dialog box, click **Yes**. After 20 to 40 seconds, a "lost node connection, changing to network view" message is displayed.

e. Click **OK**. On the network view map, the node where you reset the XTC is gray.

f. After the node icon turns green (within 1 to 2 minutes), double-click it. On the shelf graphic, observe the following:
   - The previous standby XTC displays a green ACT LED.
   - The previous active XTC LEDs go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (XTC is in standby mode).
   - The LEDs should complete this sequence within 5 to 10 minutes.

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:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the faulty XTC card. See "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the cross-connect loopback:
   - Click the **Circuits** tab.
   - Choose the cross-connect loopback circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.

d. Proceed to Step 5.

Step 4 If the test set indicates a good circuit, the XTC card might have had a temporary problem that is cleared by the switch.

Clear the cross-connect loopback:

a. Click the **Circuits** tab.

b. Choose the cross-connect loopback circuit being tested.

c. Click the **Delete** button.

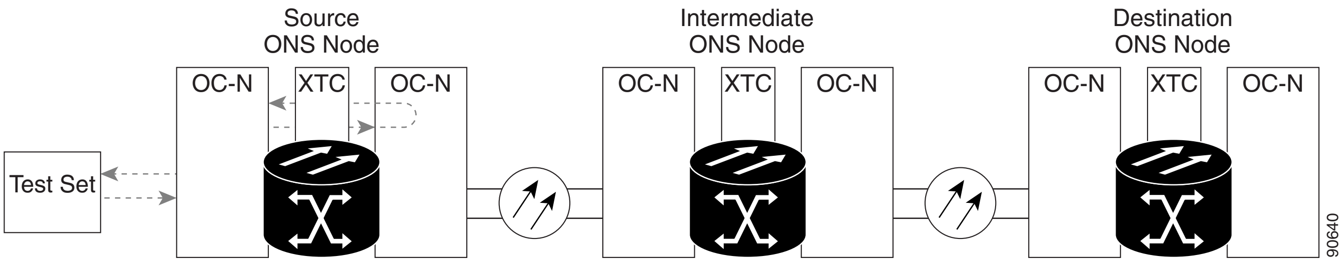
d. Click the **Yes** button in the Delete Circuits dialog box.

Step 5 Proceed to the "1.3.3 Perform a Terminal Loopback on a Source-Node OC-N Port" section on page 1-27.

1.3.3 Perform a Terminal Loopback on a Source-Node OC-N Port

The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the source node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N. Figure 1-14 shows an example of a terminal loopback on a source node OC-N port.

Figure 1-14 Terminal Loopback on a Source-Node OC-N Port



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

Procedure: Create the Terminal Loopback on a Source Node OC-N Port

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

a. If you just completed the "1.3.1 Perform a Facility Loopback on a Source-Node OC-N Port" section on page 1-22, leave the optical test set hooked up to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set hooked up to the OC-N 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 circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as OCN1toOCN2.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

e. In the Circuit Source dialog box, fill in the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the source node) and click the **Finish** button.

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

Note It is normal for a LPBKTERMINAL condition 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. 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 the **Apply** button.

f. Click the **Yes** button in the Confirmation Dialog box.

Step 5 Proceed to the "Test the Terminal Loopback Circuit" procedure on page 1-28.

Procedure: Test the Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit:

a. Clear the terminal loopback:

- Double-click the OC-N card in the source node with the terminal loopback.
- Click the **Maintenance > Loopback** tabs.
- Select **None** from the Loopback Type column for the port being tested.
- Select the appropriate state (IS, OOS, or OOS_AINS) in the State column for the port being tested.
- Click the **Apply** button.

- Click the **Yes** button in the Confirmation Dialog box.

b. Clear the terminal loopback circuit:
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

c. Proceed to the "Perform a Facility Loopback on an Intermediate-Node OC-N Port" procedure on page 1-30.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-29.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the defective OC-N card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the terminal loopback before testing the next segment of the network circuit path:
- Double-click the OC-N card in the source node with the terminal loopback.
- Click the **Maintenance > Loopback** tabs.
- Select **None** from the Loopback Type column for the port being tested.
- Select the appropriate state (IS, OOS, or OOS_AINS) in the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

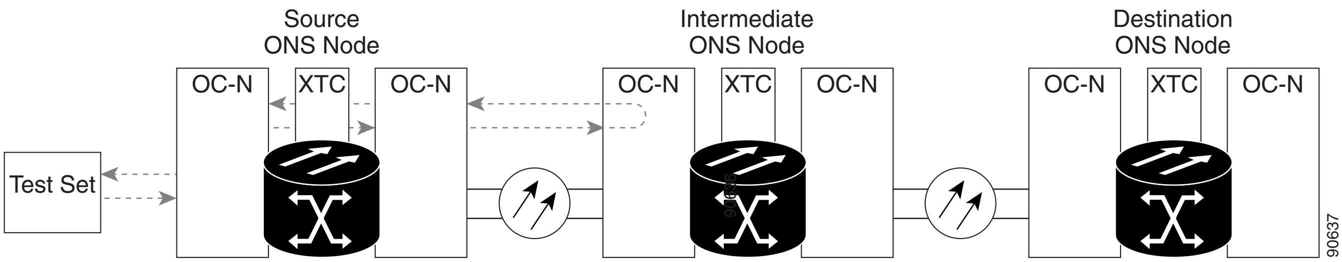
d. Clear the terminal loopback circuit before testing the next segment of the network circuit path:
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 Proceed to the "1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port" section on page 1-30.

1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port

The facility loopback test is performed on the node source port in the network circuit, in this example, the source OC-N port in the intermediate node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point. Figure 1-15 on page 1-30 shows an example of a facility loopback on a intermediate node circuit source OC-N port.

Figure 1-15 Facility Loopback on an Intermediate-Node OC-N Port



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

Procedure: Create the Facility Loopback on an Intermediate-Node OC-N Port

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

a. If you just completed the "1.3.3 Perform a Terminal Loopback on a Source-Node OC-N Port" section on page 1-27, leave the optical test set hooked up to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set hooked up to the OC-N 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 loopback circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as OCN1toOCN3.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

e. In the Circuit Source dialog box, fill in the source **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the intermediate node) and click the **Finish** button.

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

Note It is normal for a LPBKFACILITY condition to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the facility 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 the **OK** button.

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

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 the **Apply** button.

g. Click the **Yes** button in the Confirmation Dialog box.

Note It is normal for a LPBKFACILITY condition to appear during loopback setup. The condition clears when you remove the loopback.

Step 5 Proceed to the "Test the Facility Loopback Circuit" procedure on page 1-31.

Procedure: Test the Facility Loopback Circuit

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

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

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

a. Clear the facility loopback:
   - Click the **Maintenance > Loopback** tabs.
   - Choose **None** from the Loopback Type column for the port being tested.
   - Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
   - Click the **Apply** button.
   - Click the **Yes** button in the confirmation dialog box.

b. Clear the facility loopback circuit:
   - Click the **Circuits** tab.
   - Choose the loopback circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.

c. Proceed to the "1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port" section on page 1-32.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty OC-N card.

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-32.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the facility loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

d. Clear the facility loopback circuit:

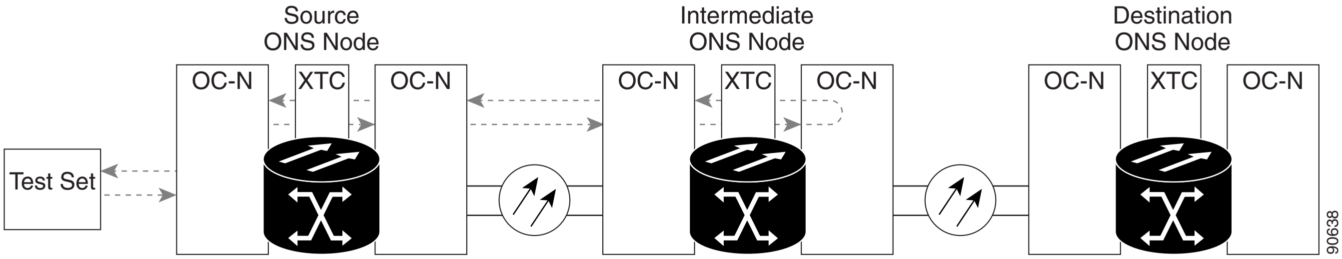
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 Proceed to the "1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port" section on page 1-32.

1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port

The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the intermediate node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N port. Figure 1-16 on page 1-33 shows an example of a terminal loopback on an intermediate node destination OC-N port.

Figure 1-16 Terminal Loopback on an Intermediate-Node OC-N Port



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

Procedure: Create the Terminal Loopback on an Intermediate-Node OC-N Port

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

a. If you just completed the "1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port" section on page 1-30, leave the optical test set hooked up to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set hooked up to the OC-N 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 circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as OCN1toOCN4.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

e. In the Circuit Source dialog box, fill in the source **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the intermediate node) and click the **Finish** button.

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

Note It is normal for a LPBKTERMINAL condition 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 the **OK** button.

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

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 the **Apply** button.

g. Click the **Yes** button in the Confirmation Dialog box.

Step 5 Proceed to the "Test the Terminal Loopback Circuit" procedure on page 1-34.

Procedure: Test the Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit:

a. Clear the terminal loopback:

- Double-click the OC-N card in the intermediate node with the terminal loopback.
- Click the **Maintenance > Loopback** tabs.
- Select **None** from the Loopback Type column for the port being tested.
- Select the appropriate state (IS, OOS, or OOS_AINS) in the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

b. Clear the terminal loopback circuit:

- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

c. Proceed to the "1.3.6 Perform a Facility Loopback on a Destination-Node OC-N Port" section on page 1-35.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-34.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the defective OC-N card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the terminal loopback:

- Double-click the OC-N card in the source node with the terminal loopback.
- Click the **Maintenance > Loopback** tabs.
- Select **None** from the Loopback Type column for the port being tested.
- Select the appropriate state (IS, OOS, or OOS_AINS) in the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

d. Clear the terminal loopback circuit:

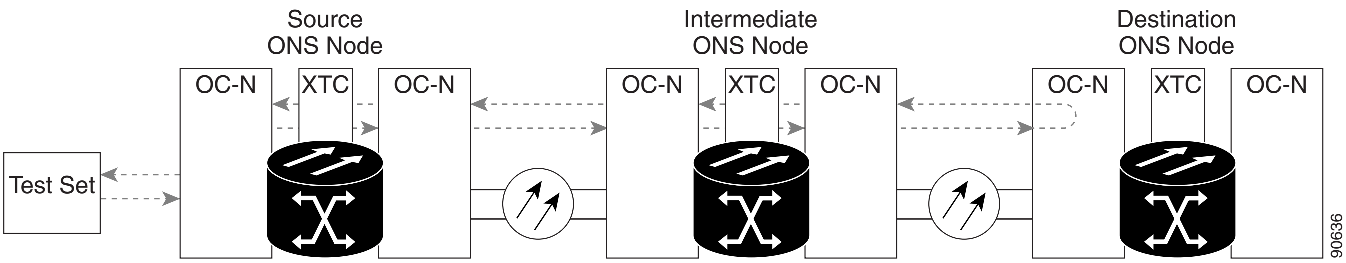
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 Proceed to the "1.3.6 Perform a Facility Loopback on a Destination-Node OC-N Port" section on page 1-35.

1.3.6 Perform a Facility Loopback on a Destination-Node OC-N Port

The facility loopback test is performed on the node source port in the network circuit, in this example, the source OC-N port in the destination node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point. Figure 1-17 shows an example of a facility loopback on a destination node circuit source OC-N port.

Figure 1-17 Facility Loopback on a Destination Node OC-N Port



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

Procedure: Create the Facility Loopback on a Destination Node OC-N Port

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

a. If you just completed the "Perform a Terminal Loopback on an Intermediate-Node OC-N Port" procedure on page 1-32, leave the optical test set hooked up to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set hooked up to the OC-N 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 loopback circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as OCN1toOCN5.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

e. In the Circuit Source dialog box, fill in the source **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the destination node) and click the **Finish** button.

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

Note It is normal for a LPBKFACILITY condition to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

- Choose **View** > **Go To Other Node** from the menu bar.
- Choose the node from the drop-down list in the Select Node dialog box and click the **OK** button.

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

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 the **Apply** button.

g. Click the **Yes** button in the Confirmation Dialog box.

Note It is normal for a LPBKFACILITY condition to appear during loopback setup. The condition clears when you remove the loopback.

Step 5 Proceed to the "Test the Facility Loopback Circuit" procedure on page 1-31.

Procedure: Test the Facility Loopback Circuit

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

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

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

a. Clear the facility loopback:
   - Click the **Maintenance > Loopback** tabs.
   - Choose **None** from the Loopback Type column for the port being tested.
   - Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
   - Click the **Apply** button.
   - Click the **Yes** button in the confirmation dialog box.

b. Clear the facility loopback circuit:
   - Click the **Circuits** tab.
   - Choose the loopback circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.

c. Proceed to the "1.3.7 Perform a Terminal Loopback on a Destination Node OC-N Port" section on page 1-38.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty OC-N card.

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-37.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the facility loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

d. Clear the facility loopback circuit:

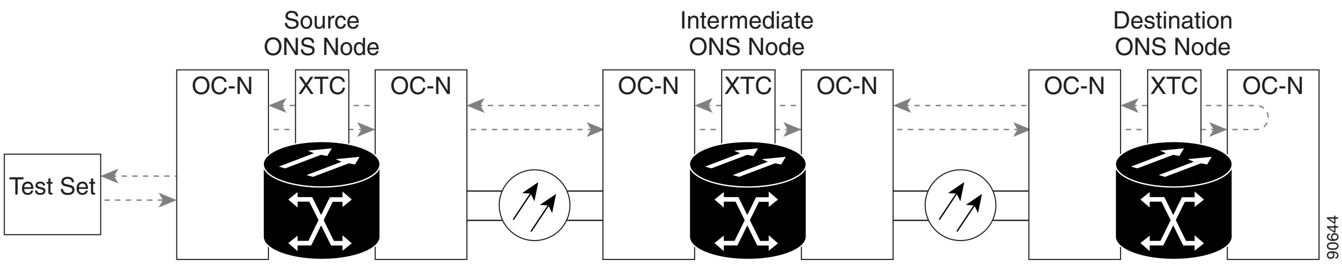
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 Proceed to the "1.3.7 Perform a Terminal Loopback on a Destination Node OC-N Port" section on page 1-38.

1.3.7 Perform a Terminal Loopback on a Destination Node OC-N Port

The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the destination node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N. Figure 1-18 shows an example of a terminal loopback on an intermediate node destination OC-N port.

Figure 1-18 Terminal Loopback on a Destination Node OC-N Port



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

Procedure: Create the Terminal Loopback on a Destination Node OC-N Port

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

a. If you just completed the "Perform a Facility Loopback on a Destination-Node OC-N Port" procedure on page 1-35, leave the optical test set hooked up to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set hooked up to the OC-N 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 circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as OCN1toOCN6.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

e. In the Circuit Source dialog box, fill in the source **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the destination node) and click the **Finish** button.

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

Note It is normal for a LPBKTERMINAL condition 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 the **OK** button.

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

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 the **Apply** button.

g. Click the **Yes** button in the Confirmation Dialog box.

Step 5 Proceed to the "Test the Terminal Loopback Circuit" procedure on page 1-40.

Procedure: Test the Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit:

a. Clear the terminal loopback:
   - Double-click the OC-N card in the intermediate node with the terminal loopback.
   - Click the **Maintenance > Loopback** tabs.
   - Select **None** from the Loopback Type column for the port being tested.
   - Select the appropriate state (IS, OOS, or OOS_AINS) in the State column for the port being tested.
   - Click the **Apply** button.
   - Click the **Yes** button in the Confirmation Dialog box.

b. Clear the terminal loopback circuit:
   - Click the **Circuits** tab.
   - Choose the loopback circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.

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

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-40.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the defective OC-N card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the terminal loopback:
   - Double-click the OC-N card in the source node with the terminal loopback.
   - Click the **Maintenance > Loopback** tabs.
   - Select **None** from the Loopback Type column for the port being tested.

- Select the appropriate state (IS, OOS, or OOS_AINS) in the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

d. Clear the terminal loopback circuit:

- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 The entire OC-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

1.4 Restoring the Database and Default Settings

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

1.4.1 Restore the Node Database

Symptom: One or more node(s) are not functioning properly or have incorrect data.

Table 1-1 on page 1-41 describes the potential cause of the symptom and the solution.

Table 1-1 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 1-41.

Procedure: Restore the Database

Note When you restore the database, the following parameters are not backed up and restored: node name, IP address, 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.

Caution E10/100-4 cards lose traffic for approximately 90 seconds when an ONS 15327 database is restored. Traffic is lost during the period of spanning-tree reconvergence. The CARLOSS alarm appears and clears during this period.

Caution If you are restoring the database on multiple nodes, wait until the XTC reboot has completed on each node before proceeding to the next node.

Step 1 Log into the node where you are restoring the database.

a. On the PC connected to the ONS 15327, start Netscape or Internet Explorer.

b. In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15327 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 display while CTC files are downloaded to your computer. The first time you connect to an ONS 15327, this process can take several minutes. After the download, the CTC Login dialog box displays.

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

Step 2 Ensure that there are no ring or span switch events; that is, ring-switch east or west, and span-switch east or west. In network view, click the **Conditions** tab and click **Retrieve Conditions** to view a list of conditions.

Step 3 If there are switch events that need to be cleared, in node (default) view, click the **Maintenance > BLSR** tabs and view the West Switch and East Switch columns.

a. If there is a switch event (not caused by a line failure), clear the switch by choosing **CLEAR** from the drop-down menu and click **Apply**.

b. If there is a switch event caused by the Wait to Restore (WTR) condition, 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's hard drive or on network storage.

Step 7 Click the database file to highlight it.

Step 8 Click **Open**. The DB Restore dialog box appears.

Caution 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 XTC card.

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.

1.4.2 Restore the Node to Factory Configuration

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

Table 1-2 describes the potential cause(s) of the symptom and the solution(s).

Table 1-2 Restore the Node to Factory Configuration

Possible Problem	Solution
Failure of both XTC cards in the node. Replacement of both XTC cards at the same time.	To restore the node to factory configuration, see the "Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" procedure on page 1-43 or the "Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" procedure on page 1-45. This procedure describes how to restore the node to factory configuration using the RE-INIT.jar JAVA file, which is referred to as the reinitialization tool in this documentation. Use this tool to upload the software package and/or restore the database after it has been backed up. You need the CD containing the latest software, the node's NE defaults, and the recovery tool.

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

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

Note If the software package files and database backup files are located in different directories, complete the Package and Database fields (Figure 1-19 on page 1-44).

Note The following parameters are not backed up and restored: node name, IP address, 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.

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

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

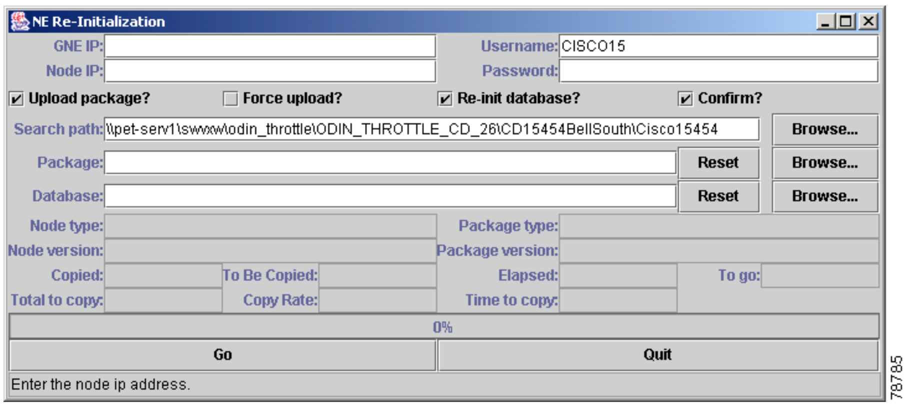
Step 1 Insert the system software CD containing the reinit tool (Figure 1-19) into the local craft interface PC drive. If the CTC Installation Wizard opens, click **Cancel**.

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 set the Files of Type drop-down menu to **All Files**.

Step 4 Select the **RE-INIT.jar** file and click **Open** to open the reinit tool (Figure 1-19).

Figure 1-19 Reinitialization Tool in Windows



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 1-19).

Step 7 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If one is not checked, click the check box.

Step 8 In the Search Path field, verify that the path to the CISCO15454 folder on the CD drive is listed.

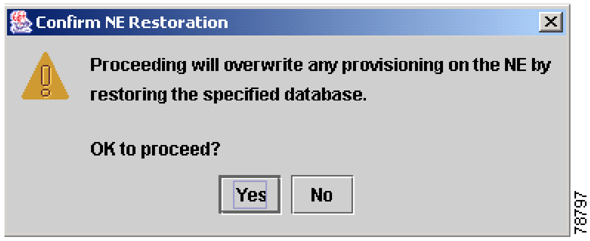
Caution Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinit tool chooses the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You might accidentally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

Caution 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 9 Click **Go**.

Step 10 A confirmation dialog box opens (Figure 1-20). Click **Yes**.

Figure 1-20 Confirm NE Restoration



Step 11 The status bar at the bottom of the window displays Complete when the node has activated the software and uploaded the database.

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

Step 12 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 XTC or on the hub or switch to which the ONS 15327 is physically connected.

Step 13 Reconnect your straight-through LAN cable to the LAN port and log back into CTC. Refer to the *Cisco ONS 15327 Procedure Guide*.

Step 14 Manually set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15327 Procedure Guide* for information on setting the node name, IP address, mask and gateway, and IIOP port.

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

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

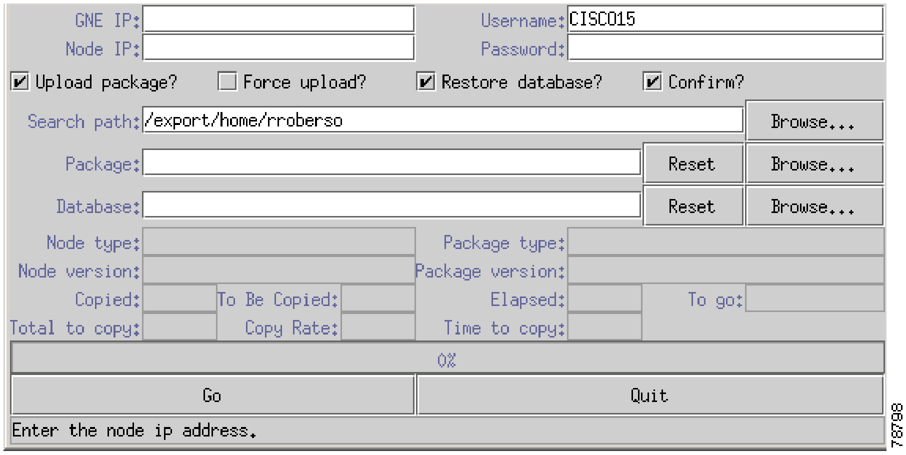
Note The XTC cards reboot several times during this procedure. Wait until they are completely rebooted before continuing.

Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the local craft interface PC drive. If the CTC Installation Wizard opens, 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 1-21). If you are working with a command line interface, run `java -jar RE-INIT.jar`.

Figure 1-21 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 1-21).

Step 6 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If any are not checked, click that check box.

Step 7 In the Search Path field, verify that the path to the CISCO15454 folder on the CD drive is listed.

> **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** 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 8 Click **Go**.

Step 9 A confirmation dialog box opens (Figure 1-20 on page 1-45). Click **Yes.**

Step 10 The status bar at the bottom of the window displays Complete when the node has activated the software and uploaded the database.

> **Note** The Complete message only indicates that the XTC successfully uploaded the database, not that the database restore is successful. The XTC then tries to restore the database after it reboots.

Step 11 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 XTC or on the hub or switch to which the ONS 15327 is physically connected.

Step 12 Reconnect your straight-through LAN cable to the LAN port and log back into CTC. Refer to the *Cisco ONS 15327 Procedure Guide*.

Step 13 Manually set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15327 Procedure Guide* for information on setting the node name, IP address, mask and gateway, and IIOP port.

1.5 PC Connectivity Troubleshooting

This section contains troubleshooting procedures for PC and network connectivity to the ONS 15327.

1.5.1 Unable to Verify the IP Configuration of Your PC

Symptom When connecting your PC to the ONS 15327, you are unable to successfully ping the IP address of your PC to verify the IP configuration.

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

Table 1-3 Unable to Verify the IP Configuration of Your PC

Possible Problem	Solution
The IP address is typed incorrectly. The IP configuration of your PC is not properly set.	Verify that the IP address used to ping the PC matches the IP address displayed when the Windows IP Configuration information is retrieved from the system. Verify the IP configuration of your PC, see the "Verify the IP Configuration of Your PC" procedure on page 1-47. If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC.

Procedure: 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 the **OK** button. The DOS command window appears.

Step 3 At the prompt in the DOS window, type one of the following appropriate commands:

- For Windows 98, NT, and 2000, type **ipconfig** and press the **Enter** key.
- For Windows 95, type **winipcfg** and press the **Enter** key.

The Windows IP configuration information is displayed, including the IP address, subnet mask, and the default gateway.

Step 4 At the prompt in the DOS window, type **ping** followed by the IP address shown in the Windows IP configuration information that you displayed in the previous step.

Step 5 Press the **Enter** key to execute the command.

If the DOS window displays 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.

1.5.2 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 1-4 describes the potential cause(s) of the symptom and the solution(s).

Table 1-4 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. See the "Reconfigure the PC Operating System Java Plug-in Control Panel" procedure on page 1-48 and the "Reconfigure the Browser" procedure on page 1-48.

Procedure: 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 Control Panel** does not appear, the JRE might not be installed on your PC.

a. Run the Cisco ONS 15327 software CD.

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

c. Double-click the **j2re-1_3_1_02-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 1.3.1_02** icon.

Step 5 Click the **Advanced** tab on the Java Plug-in Control Panel.

Step 6 From the Java Run Time Environment menu, select **JRE 1.3 in C:\ProgramFiles\JavaSoft\JRE\1.3.1_02**.

Step 7 Click the **Apply** button.

Step 8 Close the Java Plug-in Control Panel window.

Procedure: Reconfigure the Browser

Step 1 From the Start Menu, launch your browser application.

Step 2 If you are using Netscape Navigator:

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

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

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

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

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

f. Confirm that the Disk Cache Folder field shows one of the following paths:

- For Windows 95/98/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 the **Choose Folder** button.

h. Navigate to the file listed in step f and click the **OK** button.

i. Click the **OK** button 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 v1.3.1_02 for <applet> (requires restart)** check box.

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

Step 4 Temporarily disable any virus-scanning software on the computer. See the "1.6.3 Browser Stalls When Downloading CTC JAR Files from XTC" section on page 1-54.

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 into the ONS 15327.

Step 7 After completing browser configuration, enable the virus-scanning software on the computer.

1.5.3 Unable to Verify the NIC Connection on Your PC

Symptom When connecting your PC to the ONS 15327, you are unable to verify that the NIC connection is working properly because the link LED is not illuminated or flashing.

Table 1-5 describes the potential cause(s) of the symptom and the solution(s).

Table 1-5 Unable to Verify the NIC Connection on Your PC

Possible Problem	Solution
The Category 5 cable is not plugged in properly.	Confirm 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 Category 5 cable is damaged.	Ensure that the cable is in good condition. If in doubt, use a cable known to be good. Often, cabling is damaged due to pulling or bending.

Table 1-5 Unable to Verify the NIC Connection on Your PC (continued)

Possible Problem	Solution
Incorrect type of Category 5 cable is being used.	If connecting an ONS 15327 directly to your laptop/PC or a router, use a straight-through Category 5 cable. When connecting the ONS 15327 to a hub or a LAN switch, use a crossover Category 5 cable. For details on the types of Category 5 cables, see the "1.8.2.1 Crimp Replacement LAN Cables" section on page 1-74.
The NIC is improperly inserted or installed.	If you are using a PCMCIA-based NIC, remove and re-insert the NIC to make sure the NIC is fully inserted. If the NIC is built into the laptop/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 to the network (or any other node), then the NIC might be faulty and needs to be replaced.

1.5.4 Verify PC Connection to the ONS 15327 (Ping)

Symptom The TCP/IP connection is established and then lost, and a DISCONNECTED alarm appears on CTC.

Table 1-6 describes the potential cause of the symptom and the solution.

Table 1-6 Verify PC Connection to ONS 15327 (Ping)

Possible Problem	Solution
A lost connection between the PC and the ONS 15327.	Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15327 XTC card. A ping command works if the PC connects directly to the XTC card or uses a LAN to access the XTC card. See the "Ping the ONS 15327" procedure on page 1-50.

Procedure: Ping the ONS 15327

Step 1 Display the command prompt:

- **a.** If you are using a Microsoft Windows operating system, from the Start Menu choose **Run**, type **command prompt** 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-15327-IP-address
```

For example:

```
ping 192.1.0.2.
```

Step 3 If the workstation has connectivity to the ONS 15327, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a "Request timed out" message displays.

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 15327 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 15327, check that the link light on the workstation's NIC is illuminated.

1.5.5 The IP Address of the Node is Unknown

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

Table 1-7 describes the potential cause of the symptom and the solution.

Table 1-7 Retrieve the Unknown IP Address of the Node

Possible Problem	Solution
The node is not set to the default IP address.	Leave one XTC card in the shelf. Connect a PC directly to the remaining XTC card and perform a hardware reset of the XTC card. The XTC card transmits the IP address during the reset to enable you to capture the IP address for login after the XTC has completed reset. See the "Retrieve Unknown Node IP Address" procedure on page 1-51.

Procedure: Retrieve Unknown Node IP Address

Step 1 Connect your PC directly to the active XTC 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 XTC card.

Step 4 After the XTC card completes resetting, it broadcasts its IP address. The Sniffer software on your PC captures the IP address being broadcast.

1.6 CTC Operation Troubleshooting

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

1.6.1 Unable to Launch CTC Help After Removing Netscape

Symptom After removing Netscape and running CTC using Internet Explorer, the user is unable to launch the CTC Help and receives an "MSIE is not the default browser" error message.

Table 1-8 describes the potential cause of the symptom and the solution.

Table 1-8 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. Set Internet Explorer as the default browser so that CTC will associate the Help files to the correct browser. See the "Set Internet Explorer as the Default Browser for CTC" procedure on page 1-52 to associate the CTC Help files to the correct browser.

Procedure: Set 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 the **OK** button.

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.

1.6.2 Unable to Change Node View to Network View

Symptom When activating a large, multinode BLSR from Software Release 3.2 to Software Release 3.3, 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 1-9 on page 1-53 describes the potential cause of the symptom and the solution.

Table 1-9 Browser Stalls When Downloading Files From XTC

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. See the "Reset the CTC_HEAP Environment Variable for Windows" procedure on page 1-53 or the "Reset the CTC_HEAP Environment Variable for Solaris" procedure on page 1-53 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.

Procedure: 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 on **My Computer** and choose **Properties** in the shortcut menu.

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

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

Step 5 Click the **New** button under the 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.

Step 10 You can now restart the browser and CTC software.

Procedure: 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 You can now restart the browser and CTC software in the same user shell window.

1.6.3 Browser Stalls When Downloading CTC JAR Files from XTC

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

Table 1-10 describes the potential cause of the symptom and the solution.

Table 1-10 Browser Stalls When Downloading JAR File from XTC

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. See the "Disable the VirusScan Download Scan" procedure on page 1-54.

Procedure: 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 the **Configure** button 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** on the System Scan Properties dialog box.

Step 8 Click **OK** on the Task Properties window.

Step 9 Close the McAfee VirusScan window.

1.6.4 CTC Does Not Launch

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

Table 1-11 describes the potential cause of the symptom and the solution.

Table 1-11 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. See the "Redirect the Netscape Cache to a Valid Directory" procedure on page 1-55.

Procedure: Redirect the Netscape Cache to a Valid Directory

Step 1 Launch Netscape.

Step 2 Display the **Edit** menu.

Step 3 Choose **Preferences**.

Step 4 Under the Category column on the left side, expand **Advanced** and select 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.

1.6.5 Sluggish CTC Operation or Login Problems

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

Table 1-12 describes the potential cause of the symptom and the solution.

Table 1-12 Sluggish 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 15327 to download a new set of JAR files to your computer hard drive. See the "Delete the CTC Cache File Automatically" procedure on page 1-55 or the "Delete the CTC Cache File Manually" procedure on page 1-56.

Procedure: Delete the CTC Cache File Automatically

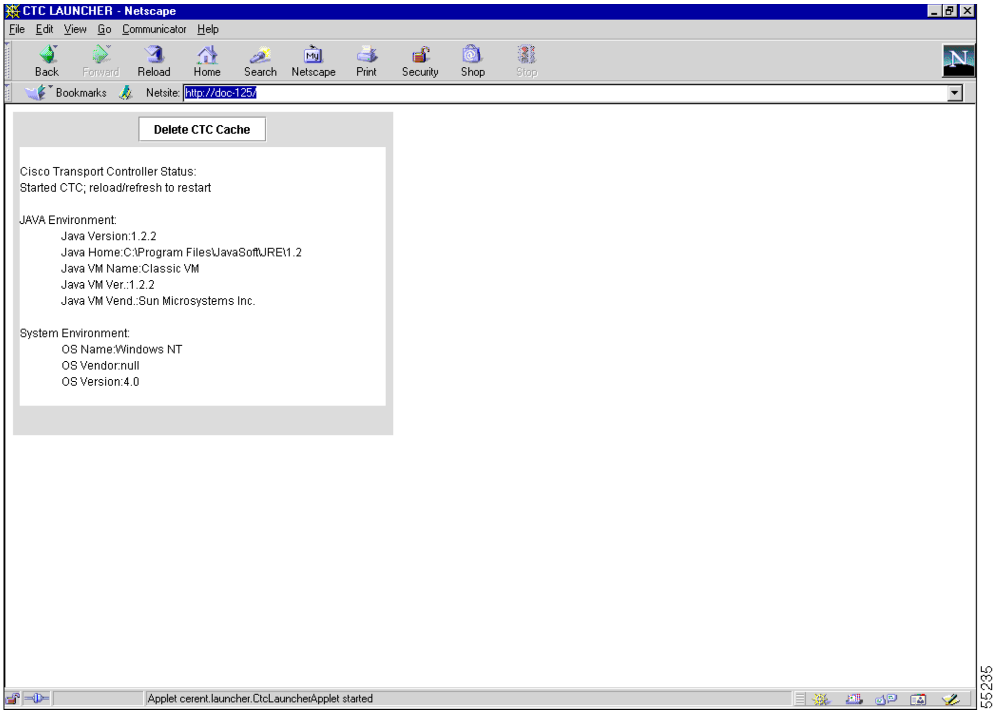
Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting the CTC cache might cause any CTC sessions running on this system to behave in an unexpected manner.

Step 1 Enter an ONS 15327 IP address in 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 the **Delete CTC Cache** button on the initial browser window to clear the CTC cache. Figure 1-22 on page 1-56 shows the Delete CTC Cache window.

Figure 1-22 Deleting the CTC Cache



Procedure: 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 on the Search Results dialog box and click **Search Now**.

Step 3 Click the **Modified** column on the Search Results dialog box to find the JAR files that match the date when you downloaded the files from the XTC. 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.

1.6.6 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 1-13 describes the potential cause(s) of the symptom and the solution(s).

Table 1-13 Node Icon is Gray on CTC Network View

Possible Problem	Solution
Different CTC releases are not recognizing each other.	Usually accompanied by an INCOMPATIBLE-SW alarm. Correct the core version build as described in the "1.6.9 Different CTC Releases Do Not Recognize Each Other" section on page 1-59.
A username/password mismatch.	Usually accompanied by a NOT-AUTHENTICATED alarm. Correct the username and password as described in the "1.6.10 Username or Password Does Not Match the XTC Information" section on page 1-60.
No IP connectivity between nodes.	Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.6.15 Ethernet Connections" section on page 1-62.
A lost DCC connection.	Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "2.6.49 EOC" section on page 2-48.

1.6.7 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 1-14 describes the potential cause(s) of the symptom and the solution(s).

Table 1-14 CTC Cannot Launch Due to Applet Security Restrictions

Possible Problem	Solution
Did not execute the javapolicyinstall.bat file. The java.policy file might be incomplete.	1. Verify that you have executed the javapolicyinstall.bat file on the ONS 15327 software CD. This file is installed when you run the CTC Setup Wizard. (Refer to the CTC installation information in the *Cisco ONS 15327 Procedure Guide* for instructions). 2. If you ran the javapolicyinstall.bat file but still receive the error message, you must manually edit the java.policy file on your computer. See the "Manually Edit the java.policy File" procedure on page 1-58.

Procedure: Manually Edit the java.policy File

Step 1 Search your computer for this 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 Windows 95, 98, and 2000 PCs, save the file to the C:\Windows folder. On Windows NT 4.0 PCs, save the file to all of the user folders on that PC, for example, C:\Winnt\profiles\joeuser.

1.6.8 Java Runtime Environment Incompatible

Symptom The CTC application does not run properly.

Table 1-15 describes the potential cause of the symptom and the solution.

Table 1-15 Java Runtime Environment Incompatible

Possible Problem	Solution
The compatible Java 2 JRE is not installed.	The Java 2 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 15327 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 15327 software CD and on the Cisco ONS 15327 documentation CD. See the "Launch CTC to Correct the Core Version Build" procedure on page 1-59. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with all of the releases that you are running. See Table 1-16 on page 1-59.

Note Software R4.0 will notify you if an older version JRE is running on your PC or UNIX workstation.

Table 1-16 on page 1-59 shows JRE compatibility with ONS 15327 software releases.

Table 1-16 JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible
ONS 15327 Release 1.0.0	Yes	No
ONS 15327 Release 1.0.1	Yes	Yes
ONS 15327 Release 2.2.1 and earlier	Yes	No
ONS 15327 Release 2.2.2	Yes	Yes
ONS 15327 Release 3.0	Yes	Yes
ONS 15327 Release 3.1	Yes	Yes
ONS 15327 Release 3.2	Yes	Yes
ONS 15327 Release 3.3	Yes	Yes
ONS 15327 Release 3.4	No	Yes
ONS 15327 Release 4.0	No	Yes

Procedure: 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 15327 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 Release 2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to both the ONS 15327 and ONS 15454, while the element files are unique to the particular product. For example, the ONS 15327 Release 1.0 uses a Version 2.3 core build and a Version 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.

1.6.9 Different CTC Releases Do Not Recognize Each Other

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

Table 1-17 on page 1-60 describes the potential cause of the symptom and the solution.

Table 1-17 Different CTC Releases Do Not Recognize Each Other

Possible Problem	Solution
The software loaded on the connecting workstation and the software on the XTC card are incompatible.	This occurs when the XTC 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 earlier and then attempt to log into another ONS node in the network running a later CTC core version, the earlier version node does not recognize the new node. See the "Launch CTC to Correct the Core Version Build" procedure on page 1-60.

Procedure: 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 In the Node Name field, type the ONS 15327 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 XTC.

1.6.10 Username or Password Does Not Match the XTC Information

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

Table 1-18 describes the potential cause(s) of the symptom and the solution(s).

Table 1-18 Username or Password Does Not Match the XTC Information

Possible Problem	Solution
The username or password entered does not match the information stored in the XTC.	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 logon to the ONS 15327, type the CISCO15 username in capital letters and click **Login** (no password is required). If you are using CTC Software Release 2.2.2 or earlier and CISCO15 does not work, type cerent454 for the username. See the "Verify Correct Username and Password" procedure on page 1-61.

Procedure: 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 to have them enter your system and create a new user name and password.

1.6.11 No IP Connectivity Exists Between Nodes

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

Table 1-19 describes the potential cause of the symptom and the solution.

Table 1-19 No IP Connectivity Exists Between Nodes

Possible Problem	Solution
Lost Ethernet connection	Usually, this condition is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.6.15 Ethernet Connections" section on page 1-62.

1.6.12 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 1-20 describes the potential cause of the symptom and the solution.

Table 1-20 DCC Connection Lost

Possible Problem	Solution
A lost DCC connection	Usually, this condition is accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "2.6.49 EOC" section on page 2-48.

1.6.13 "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 1-21 on page 1-62 describes the potential cause of the symptom and the solution.

Table 1-21 "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. See the "Cancel the Circuit Creation and Start Over" procedure on page 1-62.

Procedure: Cancel the Circuit Creation and Start Over

Step 1 Cancel the circuit creation:

- Click the **Cancel** button.
- Click the **Back** button until you return to the initial circuit creation window.

Step 2 Check the list of available ports. The previously selected port no longer appears in the available list because it is now part of a provisioned circuit.

Step 3 Select a different available port and begin the circuit creation process.

1.6.14 Calculate and Design IP Subnets

Symptom You cannot calculate or design IP subnets on the ONS 15327.

Table 1-22 describes the potential cause(s) of the symptom and the solution(s).

Table 1-22 Calculate and Design IP Subnets

Possible Problem	Solution
The IP capabilities of the ONS 15327 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 15327 IP capability, refer to the *Cisco ONS 15327 Reference Manual.*

1.6.15 Ethernet Connections

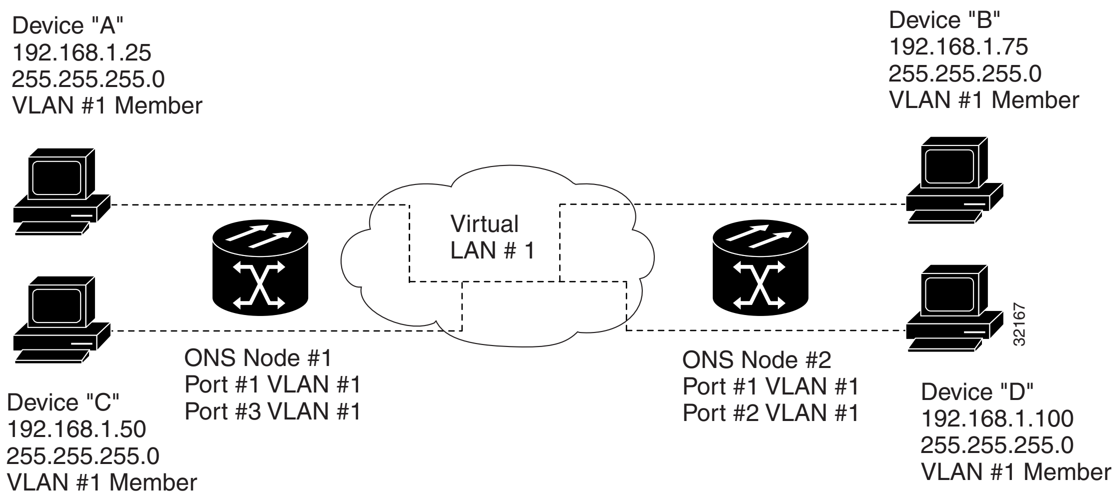
Symptom Ethernet connections appear to be broken or are not working properly.

Table 1-23 on page 1-63 describes the potential cause(s) of the symptom and the solution(s).

Table 1-23 Ethernet Connections

Possible Problem	Solution
Improperly seated connections	You can fix most connectivity problems in an Ethernet network by following a few guidelines. See Figure 1-23 when consulting the steps in the "Verify Ethernet Connections" procedure on page 1-63.
Incorrect connections	

Figure 1-23 Ethernet Connectivity Reference



Procedure: Verify Ethernet Connections

Step 1 Verify that the alarm filter is turned OFF.

Step 2 Check for SONET 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 15327 #1 and Ports 1 and 2 on ONS 15327 #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 15327s 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 an Ethernet cable known to be good.

d. Check the status LED on the Ethernet card faceplate to ensure that 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. Run the procedure in the "1.9.3 Lamp Test for Card LEDs" section on page 1-80.

Step 7 Verify connectivity between device A and device C by pinging between these locally attached devices (see the "1.5.4 Verify PC Connection to the ONS 15327 (Ping)" section on page 1-50). If the ping is unsuccessful:

a. Verify that device A and device C are on the same IP subnet.

b. Display 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 15327 #1 and ONS 15327 #2 ports also use VLAN #1.

1.6.16 VLAN Cannot Connect to Network Device from Untag Port

Symptom Networks that have a VLAN with one ONS 15327 Ethernet card port set to Tagged and one ONS 15327 Ethernet card set to Untag might have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port (Figure 1-24). 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 1-24 VLAN with Ethernet Ports at Tagged and Untag

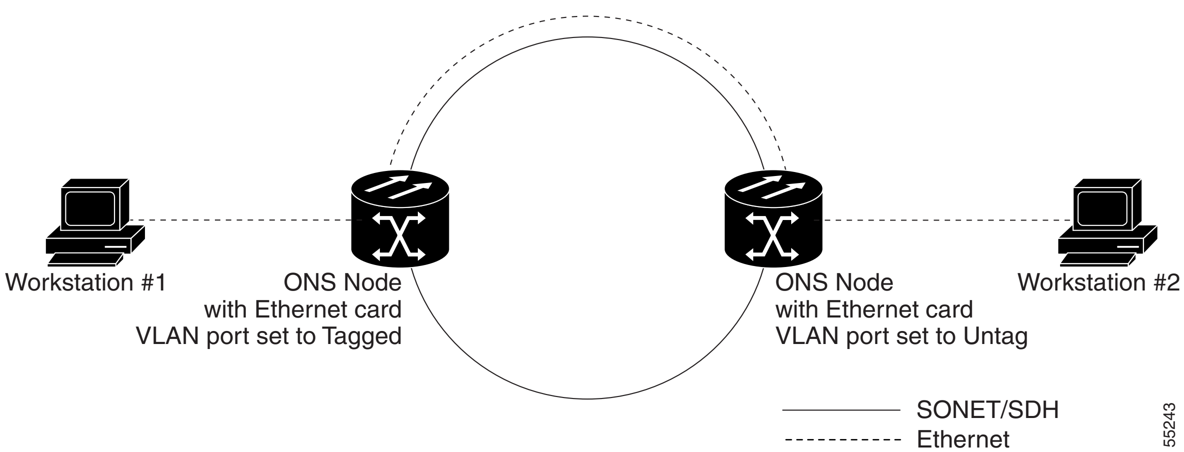


Table 1-24 on page 1-65 describes the potential cause(s) of the symptom and the solution(s).

Table 1-24 VLAN Cannot Connection to Network Device from Untag Port

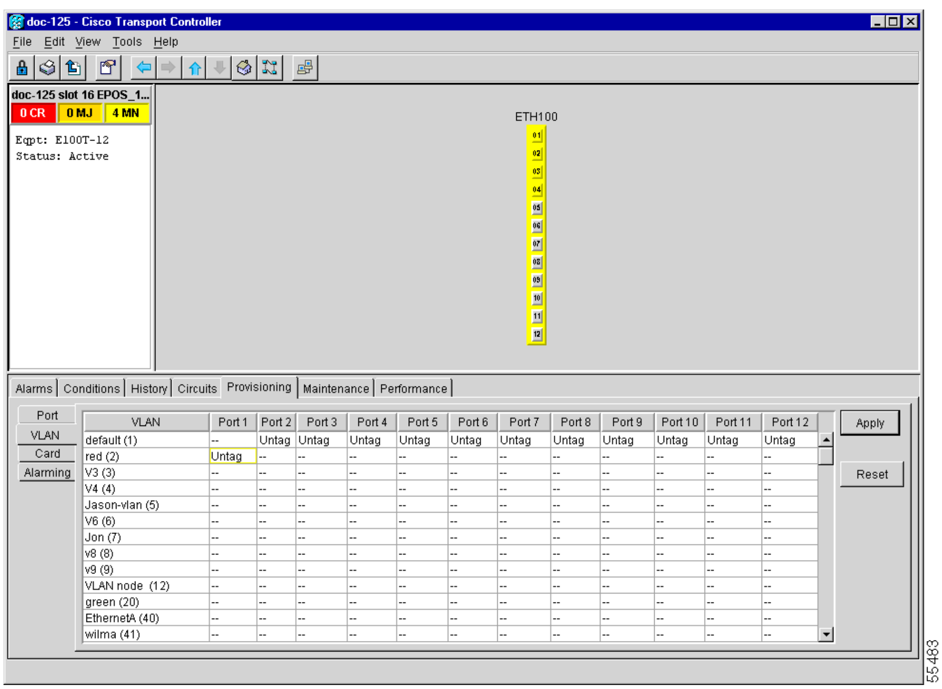
Possible Problem	Solution
The Tagged ONS 15327 adds the IEEE 802.1Q tag and the Untag ONS 15327 removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet.	See the "Change VLAN Port Tag and Untagged Settings" procedure on page 1-65. 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 prevents 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 can 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 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.	

Procedure: 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 > VLAN** tabs (Figure 1-25).

Figure 1-25 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**.

1.7 Circuits and Timing

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

1.7.1 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 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 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 circuit is in the OOS_AINS state and at least one other connection in the circuit is in IS or OOS_AINS state.

Table 1-25 describes the potential cause(s) of the symptom and the solution(s).

Table 1-25 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. Refer to the "View the State of Circuit Nodes" procedure on page 1-67. Log onto 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 15327 Software Upgrade Guide* for software upgrade procedures. **Note** If the node software cannot be upgraded to Software R4.0, the partial state condition can be avoided by only using the circuit state(s) supported in the earlier software release.

Table 1-25 Circuit in Partial State (continued)

<table>
<tr><th>Possible Problem</th><th>Solution</th></tr>
<tr><td>During an automatic transition, some path-level defects and/or alarms were detected on the circuit.</td><td rowspan="2">Determine which node in the circuit is not changing to the desired state. Refer to the "View the State of Circuit Nodes" procedure on page 1-67.

Log into 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 15327 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.</td></tr>
<tr><td>One end of the circuit is not properly terminated.</td></tr>
</table>

Procedure: View the State of Circuit Nodes

Step 1 Click the **Circuits** tab.

Step 2 From the Circuits tab list, select the circuit with the *_PARTIAL state condition.

Step 3 Click the **Edit** button. The Edit Circuit window appears.

Step 4 In the Edit Circuit window, click the **State** tab.

The State tab window lists the Node, CRS End A, CRS End B, and CRS State for each of the nodes in the circuit.

1.7.2 AIS-V on XTC-28-3 Unused VT Circuits

Symptom An incomplete circuit path causes an alarm indications signal (AIS).

Table 1-26 describes the potential cause of the symptom and the solution.

Table 1-26 AIS-V on XTC-28-3 Unused VT Circuits

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 XTC-28-3 VT circuits that are not carrying traffic and on stranded bandwidth. Perform the "Clear AIS-V on XTC-28-3 Unused VT Circuits" procedure on page 1-67.

Procedure: Clear AIS-V on XTC-28-3 Unused VT Circuits

Step 1 Determine the affected port.

Step 2 Record the node ID, slot number, port number, and 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 XTC-28-3 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 XTC-28-3 card in CTC card view. Click **Maintenance > DS1**.

Step 13 Locate the VT in Facility (line) Loopback list.

Step 14 From the Loopback Type list, choose **None** and then click **Apply**.

Step 15 Click the **Alarm** tab and verify that the AIS-V alarms have cleared.

Step 16 Repeat this procedure for all the AIS-V alarms on the XTC-28-3 cards.

1.7.3 Circuit Creation Error with VT1.5 Circuit

Symptom You might 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 1-27 describes the potential cause(s) of the symptom and the solution(s).

Table 1-27 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 15327 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 15327 Reference Manual* for more information.

1.7.4 DS3 Card Does Not Report AIS-P From External Equipment

Symptom A DS-3 card does not report STS AIS-P from the external equipment/line side.

Table 1-28 describes the potential cause of the symptom and the solution.

Table 1-28 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. DS-3 cards have DS-3 header monitoring functionality, which allows you to view performance monitoring (PM) on the DS-3 path. Nevertheless, you cannot view AIS-P on the STS path. For more information on the PM capabilities of the DS-3 cards, refer to the *Cisco ONS 15327 Procedure Guide*.

1.7.5 OC-3 and DCC Limitations

Symptom Limitations to OC-3 and DCC usage.

Table 1-29 describes the potential cause of the symptom and the solution.

Table 1-29 OC-3 and DCC Limitations

Possible Problem	Solution
OC-3 and DCC have limitations for the ONS 15327.	For an explanation of OC-3 and DCC limitations, refer to the DCC Tunnels section of the *Cisco ONS 15327 Procedure Guide*.

1.7.6 ONS 15327 Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

Table 1-30 describes the potential cause(s) of the symptom and the solution(s).

Table 1-30 ONS 15327 Switches Timing Reference

<table>
<tr><th>Possible Problem</th><th>Solution</th></tr>
<tr><td>The optical or building integrated timing supply (BITS) input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source.</td><td rowspan="7">The ONS 15327 internal clock operates at a Stratum 3 level of accuracy. This gives the ONS 15327 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} per day, including temperature.
ONS 15327 free-running synchronization relies on the Stratum 3 internal clock.
Use a higher quality Stratum 1 or Stratum 2 timing source. This results in fewer timing slips than a lower quality Stratum 3 timing source.</td></tr>
<tr><td>The optical or BITS input is not functioning.</td></tr>
<tr><td>Synchronization status message (SSM) is set to Don’t Use for Synchronization (DUS).</td></tr>
<tr><td>SSM indicates a Stratum 3 or lower clock quality.</td></tr>
<tr><td>The input frequency is off by more than 15 ppm.</td></tr>
<tr><td>The input clock wanders and has more than three slips in 30 seconds.</td></tr>
<tr><td>A bad timing reference existed for at least two minutes.</td></tr>
</table>

1.7.7 Holdover Synchronization Alarm

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

Table 1-31 describes the potential cause of the symptom and the solution.

Table 1-31 Holdover Synchronization Alarm

Possible Problem	Solution
The last reference input has failed.	The clock is running at the frequency of the last valid reference input. This alarm is raised when the last reference input fails. See the "2.6.94 HLDOVRSYNC" section on page 2-73 for a detailed description of this alarm. **Note** The ONS 15327 supports holdover timing per Telcordia GR-4436 when provisioned for external (BITS) timing.

1.7.8 Free-Running Synchronization Mode

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

Table 1-32 describes the potential cause of the symptom and the solution.

Table 1-32 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 "2.6.90 FRNGSYNC" section on page 2-71 for a detailed description of this alarm.

1.7.9 Daisy-Chained BITS Not Functioning

Symptom You are unable to daisy-chain the BITS.

Table 1-33 describes the potential cause of the symptom and the solution.

Table 1-33 Daisy-Chained BITS Not Functioning

Possible Problem	Solution
Daisy-chaining BITS is not supported on the ONS 15327.	Daisy-chaining BITS causes additional wander buildup in the network and is therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each ONS 15327.

1.7.10 Blinking STAT LED after Installing a Card

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

Table 1-34 describes the potential cause of the symptom and the solution.

Table 1-34 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-BOOT alarm is raised against the slot number with an "Equipment Fails To Boot" description. Check the alarm tab for this alarm to appear for the slot where the card is installed. To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card.

1.8 Fiber and Cabling

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

1.8.1 Bit Errors Appear for a Traffic Card

Symptom A traffic card has multiple bit errors.

Table 1-35 describes the potential cause of the symptom and the solution.

Table 1-35 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 isolates 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 15327. Troubleshoot cabling problems using the "1.1 Network Troubleshooting Tests" section on page 1-2. Troubleshoot low optical levels using the "1.8.2 Faulty Fiber-Optic Connections" section on page 1-72.

1.8.2 Faulty Fiber-Optic Connections

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

Table 1-36 describes the potential cause(s) of the symptom and the solution(s).

Table 1-36 Faulty Fiber-Optic Connections

Possible Problem	Solution
Faulty fiber-optic connections.	Faulty fiber-optic connections can be the source of SONET alarms and signal errors. See the "Verify Fiber-Optic Connections" procedure on page 1-72.
Faulty Category-5 cables.	Faulty Category-5 cables can be the source of SONET alarms and signal errors. See the "1.8.2.1 Crimp Replacement LAN Cables" section on page 1-74.
Faulty gigabit interface connectors.	Faulty gigabit interface converters can be the source of SONET alarms and signal errors. See the "1.8.2.2 Replace Faulty SFP Connectors" section on page 1-76.

Warning **Follow all directions and warning labels when working with optical fibers. To prevent eye damage, never look directly into a fiber or connector.**

Warning **Class IIIb laser.**

Warning **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.**

Warning **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.**

Procedure: Verify Fiber-Optic Connections

Step 1 Ensure that a single-mode fiber connects to the ONS 15327 card.

SM or SM Fiber should be printed on the fiber span cable. ONS 15327 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 that the power meter is set to the appropriate wavelength for the optical 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; see the "1.8.2.3 Optical Card Transmit and Receive Levels" section on page 1-77.

Step 4 If the power level falls below the specified range:

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 15327 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 15327 Procedure Guide*. If possible, do this for the 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 card to eliminate the possibility of a degrading transmitter on this card.

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 optical 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 15327 Procedure Guide*. If possible, do this for the 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 optical card.

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

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

Receiver overloads occur when maximum receiver power is exceeded.

Tip To prevent overloading the receiver, use an attenuator on the fiber between the card transmitter and the receiver. Place the attenuator on the receive transmitter of the 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.

1.8.2.1 Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the ONS 15327. Use a cross-over cable when connecting an ONS 15327 to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15327 to a router or workstation. Use #22 or #24 AWG shielded wire with RJ-45 connectors, and a crimping tool. Figure 1-26 shows the layout of an RJ-45 connector.

Figure 1-26 RJ-45 Pin Numbers

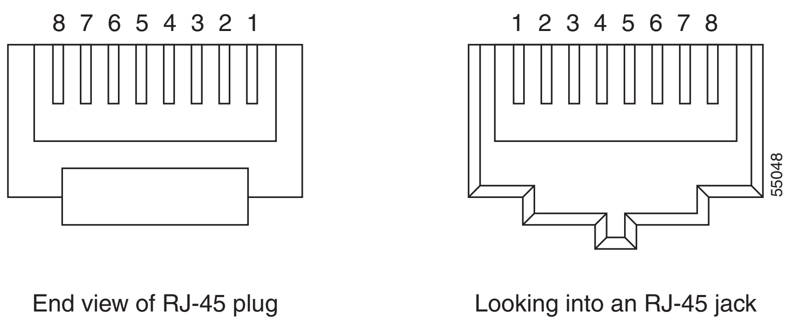


Figure 1-27 shows the layout of a LAN cable.

Figure 1-27 LAN Cable Layout

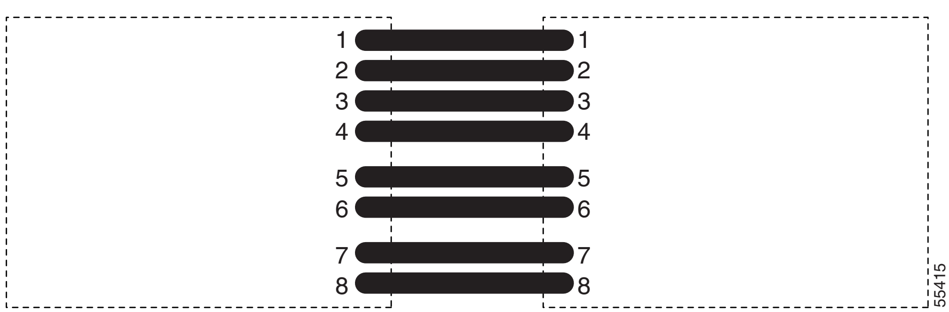


Table 1-37 shows the pinout of a LAN cable.

Table 1-37 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 1-28 on page 1-75 shows the layout of a cross-over cable.

Figure 1-28 Cross-Over Cable Layout

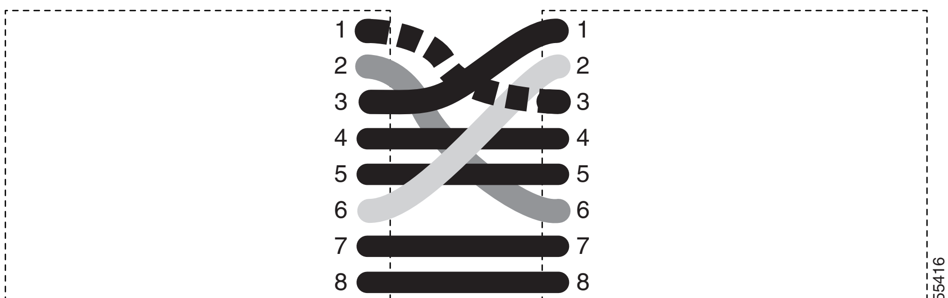


Table 1-38 shows the pinout of a cross-over cable.

Table 1-38 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.

1.8.2.2 Replace Faulty SFP Connectors

Small Form-factor Pluggable (SFP) connectors are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

Warning **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.**

SFPs are input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. The type of SFP determines the maximum distance that the Ethernet traffic can travel from the card to the next network device. For a description of SFPs and their capabilities, see Table 1-39 on page 1-76 and refer to the *Cisco ONS 15327 Reference Manual*.

Note SFPs must be matched on either end by type: SX to SX, LX to LX.

Table 1-39 Available SFP Connectors

SFP	Associated Cards	Application	Fiber	Product Number
1000BaseSX	G1000-2	Short reach	Multimode fiber up to 550 m long	15327-SFP-LC-SX=
1000BaseLX	G1000-2	Long reach	Single-mode fiber up to 5 km long	15327-SFP-LC-LX=

Procedure: Remove SFP Connectors

Step 1 Disconnect the network fiber cable from the 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 SFP from the slot by simultaneously squeezing the two plastic tabs on each side.

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

Procedure: Install SFP Connectors

Step 1 Remove the SFP from its protective packaging.

Step 2 Check the label to verify that the SFP is the correct type (SX or LX) for your network.

Step 3 Verify that you are installing compatible SFPs; for example, SX to SX, LX to LX.

Step 4 Grip the sides of the SFP with your thumb and forefinger and insert the SFP into the slot on the G1000-2 card.

Note SFPs are keyed to prevent incorrect installation.

Step 5 Slide the SFP through the flap that covers the opening until you hear a click. The click indicates the SFP is locked into the slot.

Step 6 When you are ready to attach the network fiber-optic cable, remove the protective plug from the SFP and save the plug for future use.

1.8.2.3 Optical Card Transmit and Receive Levels

Each G1000-2 and OC-N card has a transmit and receive connector on its faceplate. Table 1-40 describes the SFPs and their capabilities.

Table 1-40 Optical Card Transmit and Receive Levels

Optical Card	Receive	Transmit
G1000-2	–8 to –28 dBm	–8 to –15 dBm
OC3 IR 4 1310	–8 to –28 dBm	–8 to –15 dBm
OC12 IR 1310	–8 to –28 dBm	–8 to –15 dBm
OC12 LR 1550	–8 to –28 dBm	+2 to –3 dBm
OC48 IR 1310	0 to –18 dBm	0 to –5 dBm
OC48 LR 1550	–8 to –28 dBm	+3 to –2 dBm

1.9 Power and LED Tests

This section provides symptoms and solutions for power supply problems, power consumption, and LED indicators.

1.9.1 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 1-41 describes the potential cause(s) of the symptom and the solution(s).

Table 1-41 Power Supply Problems

Possible Problem	Solution
Loss of power or low voltage Improperly connected power supply	The ONS 15327 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 15327 that is not properly connected to its power supply does not operate. Power problems can be confined to a specific ONS 15327 or can affect several pieces of equipment on the site. **Note** A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15327 to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning > General** tabs and change the Date and Time fields. See the "Isolate the Cause of Power Supply Problems" procedure on page 1-79.

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 15327. 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 15327 are service-affecting.

Procedure: Isolate the Cause of Power Supply Problems

Step 1 If a single ONS 15327 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 15327 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 brown-outs 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.

1.9.2 Power Consumption for Node and Cards

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

Table 1-42 describes the potential cause of the symptom and the solution.

Table 1-42 Power Consumption for Node and Cards

Possible Problem	Solution
Improper power supply.	Refer to power information in the *Cisco ONS 15327 Procedure Guide*.

1.9.3 Lamp Test for Card LEDs

Symptom Card LED does not light or you are unsure if LEDs are working properly.

Table 1-43 describes the potential cause of the symptom and the solution.

Table 1-43 Lamp Test for Card LEDs

Possible Problem	Solution
Faulty LED	A lamp test verifies that all the card LEDs work. Run this diagnostic test as part of the initial ONS 15327 turn-up, a periodic maintenance routine, or any time you question whether an LED is in working order. See the "Verify Card LED Operation" procedure on page 1-80.

Procedure: Verify Card LED Operation

Step 1 Click the **Maintenance > Diagnostic** tabs.

Step 2 Click **Lamp Test**.

Step 3 Watch to make sure all the LEDs on the cards illuminate for several seconds.

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

If an LED does not light up, the LED is faulty. Call the Cisco TAC and fill out an RMA to return the card.