General Troubleshooting

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 15310-CL. To troubleshoot specific ONS 15310-CL alarms, see Chapter 2, “Alarm Troubleshooting.” If you cannot find what you are looking for, contact the Cisco Technical Assistance Center (TAC). For more information, see the “Obtaining Technical Assistance” section on page xxxii.

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.
- **1.2 Identify Points of Failure on an Electrical Circuit Path**—Explains how 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**—Explains how to perform loopback and hairpin tests, which you can use to test OC-N circuit paths through the network or logically isolate faults.
- **1.4 Restore the Database and Default Settings**—Explains how to restore software data and restore the node to the default setup.
- **1.5 PC Connectivity Troubleshooting**—Provides troubleshooting procedures for PC and network connectivity to the ONS 15310-CL.
- **1.6 CTC Operation Troubleshooting**—Provides troubleshooting procedures for Cisco Transport Controller (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.
1.1 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. 15310-CL-CTX DS-1, DS-3, EC-1, and OC-3 optical ports in addition to CE-100T-8 cards allow loopbacks and hairpin circuits. ML-100T-8 Ethernet cards do not allow loopbacks.

**Caution**
On OC-N ports, a facility loopback applies to the entire port and not an individual circuit. Exercise caution when using loopbacks on an OC-N port carrying live traffic.

### 1.1.1 Facility Loopback

A facility loopback tests the line interface unit (LIU) of the card 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 15310-CL-CTX LIU or the cabling plant as the potential cause of a network problem.

**Caution**
Before performing a facility loopback on an OC-N port, make sure there are at least two data communications channel (DCC) paths to the node where the 15310-CL-CTX 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 15310-CL containing the loopback OC-N port.

### 1.1.2 Terminal Loopback

A terminal loopback tests a circuit path as it passes through the 15310-CL-CTX of the ONS 15310-CL and loops back from the port with the loopback. A terminal loopback on an OC-N port turns the signal around before it reaches the LIU and sends it back through the 15310-CL-CTX. This test verifies that the 15310-CL-CTX cross-connect circuit paths are valid.

For a CE-100T-8 card, the test-set traffic comes in on the ONS 15310-CL DS-3 port and goes through the 15310-CL-CTX to an OC-N port. The terminal loopback on the OC-N port turns the signal around before it reaches the LIU and sends it back through the 15310-CL-CTX to the electrical port. This test verifies that the port cross-connect circuit paths are valid, but does not test the LIU on the OC-N port.

### 1.1.3 Hairpin Circuit

A hairpin circuit brings traffic in and out on an electrical port instead of sending the traffic onto the OC-N line. A hairpin loops back only the specific synchronous transport signal (STS) or virtual tributary (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.
1.1.4 Cross-Connect Loopback

A cross-connect loopback tests a circuit path as it passes through the cross-connect portion of the 15310-CL-CTX 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 on an optical facility without interrupting the other STS circuits.

You can create a cross-connect loopback on working or protect OC-3 optical ports unless the protect port is used in a 1+1 protection group and is in working mode.

---

**Note**

If a terminal or facility loopback exists on an optical port, you cannot use the cross-connect loopback.

1.2 Identify Points of Failure on an Electrical 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 tests in this section can be used to test a DS-1, DS-3, or EC-1 circuit on a path protection. 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 port
2. Hairpin on the source-node port
3. Terminal loopback to the destination-node port
4. Hairpin on the destination-node port
5. Facility loopback to the destination port

---

**Note**

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

**Note**

Facility and terminal loopback tests require on-site personnel.

**Note**

These procedures are performed when power connections to the nodes or sites are 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 Port

The facility loopback test is performed on the node source port in the network circuit. Completing a successful facility loopback on this port isolates the cabling and port as possible failure points.

---

**Caution**

Performing a loopback on an in-service circuit is service-affecting.
1.2.1 Perform a Facility Loopback on a Source Port

Note Loopbacks operate only on ports in the out-of-service, maintenance (OOS,MT) Admin State and out-of-service and Management, Maintenance (OOS-MA,MT) service state.

Create the Facility Loopback on the Source Port

**Step 1**
Connect an electrical test set to the ONS 15310-CL DS-3 port you are testing.
Use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the port.

**Step 2**
Adjust the test set accordingly.

**Step 3**
Use CTC to create the facility loopback on the port being tested:
   a. In node view, double-click the 15310-CL-CTX card where you are performing the loopback.
   b. According to the circuit type you want to check, click one of the following tabs:
      - DS1 > Maintenance > Loopback
      - DS3 > Maintenance > Loopback
      - EC1 > Maintenance > Loopback
   c. Choose **OOS,MT** from the Admin State column for the port being tested.
   d. Choose **Facility (Line)** from the Loopback Type column for the port being tested.
   e. Click **Apply**.
   f. Click **Yes** in the confirmation dialog box.

Note It is normal for a facility loopback (LPBKFAI) condition to appear during loopback setup. The condition clears when you remove the loopback.

**Step 4**
Continue with the “Test the Facility Loopback” procedure on page 1-4.

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, clear the loopback:
   a. According to the circuit type you want to clear, click one of the following tabs:
      - DS1 > Maintenance > Loopback
      - DS3 > Maintenance > Loopback
      - EC1 > Maintenance > Loopback
   b. Choose **None** from the Loopback Type column for the port being tested.
c. Choose the appropriate state (IS,AUNS; OOS,DSBLD; or OOS,MT) from the Admin State column for the port being tested.

d. Click Apply.

e. Click Yes in the confirmation dialog box.

**Step 4**

If the test set indicates a faulty circuit, the problem might be a faulty 15310-CL-CTX, faulty port, or faulty cabling from the DS-3 port. Continue with the “Test the Electrical Cabling” procedure on page 1-5.

---

**Test the Electrical Cabling**

**Step 1**

Replace the suspect cabling (the cables from the test set to the DS-1, DS-3, or EC-1 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 electrical port 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. Replace the defective cable, then clear the loopback:

a. According to which circuit type you want to clear, click one of the following tabs:
   - DS1 > Maintenance > Loopback
   - DS3 > Maintenance > Loopback
   - EC1 > Maintenance > Loopback

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

c. Choose the appropriate state (IS,AUNS; OOS,DSBLD; or OOS,MT) from the Admin State column for the port being tested.

d. Click Apply.

e. Click Yes in the confirmation dialog box.

**Step 4**

If the test set indicates a faulty circuit, the problem might be a faulty port. Continue with the “1.2.2 Perform a Hairpin on a Source Node Port” procedure on page 1-5.

---

**1.2.2 Perform a Hairpin on a Source Node Port**

The hairpin test is performed on the first port in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through this port isolates the possibility that the source port is the cause of the faulty circuit.
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 “1.2.1 Perform a Facility Loopback on a Source Port” procedure on page 1-3, leave the electrical test set connected to the electrical port.
- If you are starting the current procedure without the electrical test set connected to the electrical port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the electrical connectors for the port you are testing.

Step 2  Adjust the test set accordingly.

Step 3  Use CTC to set up the hairpin on the port being tested:

a. Click the Circuits tab and click Create.

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 Next.

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

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

Step 4  Confirm that the newly created circuit appears on the Circuits tab list as a one-way circuit.

Step 5  Continue with the “Test the Hairpin Circuit” procedure on page 1-6.

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.

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

Step 4  If the test set indicates a faulty circuit, there might be a problem with the port. Continue with the “1.2.3 Perform a Terminal Loopback on a Destination Port” procedure on page 1-7.
1.2.3 Perform a Terminal Loopback on a Destination Port

The terminal loopback test is performed on the node destination port in the circuit (in this example, the port in the destination node). First, create a bidirectional circuit that starts on the source node electrical port (DS-1, DS-3, or EC-1) and terminates on the destination-node electrical port. Then continue with the terminal loopback test. Completing a successful terminal loopback to a destination-node port verifies that the circuit is good up to the destination port.

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

Create the Terminal Loopback on a Destination Port

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

a. If you just completed the “1.2.2 Perform a Hairpin on a Source Node Port” procedure on page 1-5, leave the electrical test set connected to the electrical port in the source node.

b. If you are starting the current procedure without the electrical test set connected to the ONS 15310-CL, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the connectors for the DS-3 port you are testing.

Step 2
Adjust the test set accordingly.

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

a. Click the Circuits tab and click Create.

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 Next.

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

f. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the electrical port in the destination node) and click Finish.

Step 4
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 admin state.

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

Step 5
Create the terminal loopback on the destination port being tested:

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

• From the View menu, choose Go To Other Node.

• Choose the node from the drop-down list in the Select Node dialog box and click OK.

b. In node view, double-click the 15310-CL-CTX card.
1.2.3 Perform a Terminal Loopback on a Destination Port

c. According to the circuit type you want to test, click one of the following tabs:
   - DS1 > Maintenance > Loopback
   - DS3 > Maintenance > Loopback
   - EC1 > Maintenance > Loopback

d. Select OOS,MT from the Admin State column.

e. Select Terminal (Inward) from the Loopback Type column.

f. Click Apply.

g. Click Yes in the confirmation dialog box.

---

Step 6 Continue with the “Test the Terminal Loopback Circuit on the Destination Port” procedure on page 1-8.

---

Test the Terminal Loopback Circuit on the Destination 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. Clear the terminal loopback:

a. Double-click the 15310-CL-CTX in the destination node with the terminal loopback.

b. According to the circuit type you want to clear, click one of the following tabs:
   - DS1 > Maintenance > Loopback
   - DS3 > Maintenance > Loopback
   - EC1 > Maintenance > Loopback

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

d. Select the appropriate state (IS,AINS,AINS OOS,DSBLD or OOS,MT) in the Admin State column for the port being tested.

e. Click Apply.

f. Click Yes in the confirmation dialog box.

**Step 4** Clear the terminal loopback circuit:

a. Click the Circuits tab.

b. Choose the loopback circuit being tested.

c. Click Delete.

d. Click Yes in the Delete Circuits dialog box.

**Step 5** If the test set indicates a faulty circuit, the problem might be a faulty port. Continue with the “1.2.4 Perform a Hairpin Test on a Destination-Node Port” procedure on page 1-9.
1.2.4 Perform a Hairpin Test on a Destination-Node Port

The hairpin test is performed on the port in the destination node. To perform this test, you must also create a bidirectional circuit from the destination ONS 15310-CL to the source node in the transmit direction. Creating the bidirectional circuit and completing a successful hairpin isolates the possibility that the source and destination OC-N ports, the source and destination electrical ports, or the fiber span is responsible for the faulty circuit.

Create the Hairpin Loopback Circuit on the Destination-Node Port

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Connect an electrical test set to the 15310-CL-CTX port you are testing. Use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the electrical cabling panel for the port you are testing.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Adjust the test set accordingly.</td>
</tr>
</tbody>
</table>
| **Step 3** | Use CTC to set up the source loopback circuit on the port being tested:  
  a. Click the **Circuits** tab and click **Create**.  
  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 **Next**.  
  e. In the Circuit Source dialog box, fill in the source Node, Slot, Port, and Type where the test set is connected and click **Next**.  
  f. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the port in the destination node) and click **Finish**. |
| **Step 4** | Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit. |
| **Step 5** | 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 DS-3 port on the source node is one end of the fiber span, and a DS-3 port on the destination node is the other end.  
  a. Click the **Circuits** tab and click **Create**.  
  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 **Next**.  
  e. In the Circuit Source dialog box, select the same Node, Slot, Port, and Type where the previous circuit is connected and click **Next**.  
  f. In the Circuit Destination dialog box, use the same Node, Slot, Port, and Type used for the Circuit Source dialog box and click **Finish**.  

**Step 6** | Confirm that the newly created circuit appears on the Circuits tab list as a one-way circuit. |
1.2.5 Perform a Facility Loopback on a Destination Port

Step 7 Verify that the circuits connect to the correct slots. For example, verify that source node OC-N port (east slot) is connected to the destination node (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 8 Continue with the “Test the Hairpin Circuit” procedure on page 1-10.

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; clear the hairpin circuit:
   a. Click the Circuits tab.
   b. Choose the hairpin circuit being tested.
   c. Click Delete.
   d. Click Yes in the Delete Circuits dialog box.
   e. Confirm that the hairpin circuit is deleted from the Circuits tab list.
   f. Continue with the “1.2.5 Perform a Facility Loopback on a Destination Port” procedure on page 1-10.

1.2.5 Perform a Facility Loopback on a Destination Port

The facility loopback test is performed on the last port in the circuit, in this case the port in the destination node. Completing a successful facility loopback on this port isolates the possibility that the destination-node cabling, 15310-CL-CTX, or line interface is responsible for a faulty circuit.

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.

Create a Facility Loopback Circuit on a Destination Port

Step 1 Connect an electrical test set to the port you are testing:
   a. If you just completed the “1.2.4 Perform a Hairpin Test on a Destination-Node Port” procedure on page 1-9, leave the electrical test set connected to the electrical port in the destination node.
   b. If you are starting the current procedure without the electrical test set connected to the electrical port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel.
Step 2 Use CTC to create the facility loopback on the port being tested:
   a. In node view, double-click the port where you are performing the loopback.
   b. According to the circuit type you want to check, click one of the following tabs:
      - DS1 > Maintenance > Loopback
      - DS3 > Maintenance > Loopback
      - EC1 > Maintenance > Loopback
   c. Select Facility (Line) from the Loopback Type column for the port being tested. If this is a multiport, select the row appropriate for the desired port.
   d. Click Apply.
   e. Click Yes in the confirmation dialog box.

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

Step 3 Continue with the “Test the Facility Loopback Circuit” procedure on page 1-11.

### 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:
   b. According to the circuit type you want to clear, click one of the following tabs:
      - DS1 > Maintenance > Loopback
      - DS3 > Maintenance > Loopback
      - EC1 > Maintenance > Loopback
   c. Choose None from the Loopback Type column for the port being tested.
   d. Choose the appropriate state (IS,AINS; OOS,DSBLD; or OOS,MT) from the Admin State column for the port being tested.
   e. Click Apply.
   f. Click Yes in the confirmation dialog box.

The entire electrical 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 15310-CL-CTX or faulty cabling. Continue with the “Test the Electrical Cabling” procedure on page 1-12.
1.3 Identify Points of Failure on an OC-N Circuit Path

Test the Electrical Cabling

**Step 1** Replace the suspect cabling (the cables from the test set to the DS-1, DS-3, or EC-1 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 electrical port 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. Replace the defective cable.

**Step 4** Clear the facility loopback:

a. According to the circuit type you want to clear, click one of the following tabs:
   - DS1 > Maintenance > Loopback
   - DS3 > Maintenance > Loopback
   - EC1 > Maintenance > Loopback

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

c. Choose the appropriate state (IS,AINS; OOS,DSBLD; or OOS,MT) from the Admin State column for the port being tested.

d. Click Apply.

e. Click Yes in the confirmation dialog box.

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

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

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.

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

a. In node view, double-click the 15310-CL-CTX to display the card view.

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

c. Choose **OOS,MT** from the Admin State column for the port being tested.

d. Choose **Facility (Line)** from the Loopback Type column for the port being tested.

e. Click **Apply**.

f. Click **Yes** 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** Continue with the “Test the Facility Loopback Circuit” procedure on page 1-13.

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. Clear the facility loopback:

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

b. Choose **None** from the Loopback Type column for the port being tested.
c. Choose the appropriate state (IS,AINS; OOS,DSBLD; or OOS,MT) from the Admin State column for the port being tested.
d. Click Apply.
e. Click Yes in the confirmation dialog box.
f. Continue with the “1.3.2 Perform a Cross-Connect Loopback on the Source OC-N Port” procedure on page 1-14.

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

The cross-connect loopback test occurs on the cross-connect portion of the 15310-CL-CTX in a network circuit. Completing a successful cross-connect loopback through the 15310-CL-CTX isolates the possibility that the cross-connect is the cause of the faulty circuit.

Create the Cross-Connect Loopback on the 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” procedure on page 1-13, leave the optical test set connected to the OC-N port in the source node.
b. If you are starting the current procedure without the optical test set connected 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.
c. Adjust the test set accordingly.

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

a. In node view, click the Circuits tab.
b. Click the circuit and then click Edit.
c. In the Edit Circuit dialog box, click the State tab.
d. Choose OOS-MT from the Target Circuit Admin State drop-down list.
e. Click Apply.
f. 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 node view, double-click the 15310-CL-CTX card to open the card view.
b. For the OC-N port, click the Maintenance > Optical > Loopback > SONET STS tabs.
c. Click the check box in the XC Loopback column for the port being tested.
d. Click Apply.
e. Click Yes in the confirmation dialog.

**Step 4** Continue with the “Test the Cross-Connect Loopback Circuit” procedure on page 1-15.
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 continue 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. Performing a loopback on an in-service circuit is service-affecting.

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

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

- If you just completed the “1.3.2 Perform a Cross-Connect Loopback on the Source OC-N Port” procedure on page 1-14, leave the optical test set connected to the OC-N port in the source node.
- If you are starting the current procedure without the optical test set connected 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.
- Adjust the test set accordingly.

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

- Click the Circuits tab and click Create.
- Give the circuit an easily identifiable name, such as OCN1toOCN2.
- Set circuit Type and Size to the normal preferences.
- Verify that Bidirectional is checked.
- Click Next.
1.3.3 Perform a Terminal Loopback on a Source-Node OC-N Port

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

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

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 port that requires the loopback, such as the destination OC-N port in the source node.

b. Click the Maintenance > Loopback tabs.

c. Select OOS,MT from the Admin State column.

d. Select Terminal (Inward) from the Loopback Type column.

e. Click Apply.

f. Click Yes in the confirmation dialog box.

Step 5 Continue with the “Test the Terminal Loopback Circuit” procedure on page 1-16.

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 port 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,AINS; OOS,DSBLD; or OOS,MT) in the Admin State column for the port being tested.
   - Click Apply.
   - Click Yes in the confirmation dialog box.

b. Clear the terminal loopback circuit:
   - Click the Circuits tab.
   - Choose the loopback circuit being tested.
   - Click Delete.
   - Click Yes in the Delete Circuits dialog box.
Step 4 If the test set indicates a faulty circuit, the problem might be a faulty port. Continue with the “1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port” procedure on page 1-17.

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.

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

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” procedure on page 1-15, leave the optical test set connected to the OC-N port in the source node.
   b. If you are starting the current procedure without the optical test set connected 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.
   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 Create.
   b. Give the circuit an easily identifiable name, such as OCN1toOCN3.
   c. Set circuit Type and Size to the normal preferences.
   d. Verify that Bidirectional is checked and click Next.
   e. In the Circuit Source dialog box, fill in the source Node, Slot, Port, and Type where the test set is connected and click Next.
   f. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the OC-N port in the intermediate node) and click Finish.

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 LPBFACILITY 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:
      • From the View menu, choose Go To Other Node.
      • Choose the node from the drop-down list in the Select Node dialog box and click OK.
   b. In node view, double-click the 15310-CL-CTX to display the card view and the Optical tab for OC-N ports in the intermediate node.
1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port

c. Click the Maintenance > Loopback tabs.
d. Select OOS,MT from the Admin State column.
e. Select Terminal (Inward) from the Loopback Type column.
f. Click Apply.
g. Click Yes in the confirmation dialog box.

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

Step 5 Continue with the “Test the Facility Loopback Circuit” procedure on page 1-18.

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,AINS; OOS,DSBLD; or OOS,MT) from the Admin State column for the port being tested.
      • Click Apply.
      • Click Yes in the confirmation dialog box.
   b. Clear the facility loopback circuit:
      • Click the Circuits tab.
      • Choose the loopback circuit being tested.
      • Click Delete.
      • Click Yes in the Delete Circuits dialog box.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty OC-N port. Continue with the “1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port” procedure on page 1-19.
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 continue 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.

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

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” procedure on page 1-17, leave the optical test set connected to the OC-N port in the source node.
   b. If you are starting the current procedure without the optical test set connected 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.
   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 Create.
   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 Next.
   e. In the Circuit Source dialog box, fill in the source Node, Slot, Port, and Type where the test set is connected and click Next.
   f. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the OC-N port in the intermediate node) and click Finish.

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:
      • From the View menu, choose Go To Other Node.
      • Choose the node from the drop-down list in the Select Node dialog box and click OK.
   b. In node view, double-click the 15310-CL-CTX card with the OC-N port requiring a loopback, such as the 15310-CL-CTX in the intermediate node ONS 15310-CL.
   c. Click the Maintenance > Loopback tabs.
   d. Select OOS,MT from the Admin State column.
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.

Caution
Performing a loopback on an in-service circuit is service-affecting.
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 “1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port” procedure on page 1-19, leave the optical test set connected to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set connected 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.

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 **Create**.

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 **Next**.

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

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

**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:

   - From the **View** menu, choose **Go To Other Node**.
   - Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the 15310-CL-CTX card with the OC-N port that requires the loopback, such as the 15310-CL-CTX in the destination ONS 15310-CL node.

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

d. Select **OOS,MT** from the Admin State column.

e. Select **Terminal (Inward)** from the Loopback Type column.

f. Click **Apply**.

g. Click **Yes** 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** Continue with the “Test the Facility Loopback Circuit” procedure on page 1-22.
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,AINS; OOS,DSBLD; or OOS,MT) from the Admin State column for the port being tested.
      • Click Apply.
      • Click Yes in the confirmation dialog box.
   b. Clear the facility loopback circuit:
      • Click the Circuits tab.
      • Choose the loopback circuit being tested.
      • Click Delete.
      • Click Yes in the Delete Circuits dialog box.
Step 4 If the test set indicates a faulty circuit, the problem might be a faulty OC-N port. Continue with the “1.3.7 Perform a Terminal Loopback on a Destination-Node OC-N Port” procedure on page 1-22.

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 continue 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.

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

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 “1.3.6 Perform a Facility Loopback on a Destination-Node OC-N Port” procedure on page 1-20, leave the optical test set connected to the OC-N port in the source node.
   b. If you are starting the current procedure without the optical test set connected 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.
   c. Adjust the test set accordingly.
1.3.7 Perform a Terminal Loopback on a Destination-Node OC-N Port

**Step 2** Use CTC to set up the terminal loopback circuit on the port being tested:
- a. Click the **Circuits** tab and click **Create**.
- 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 **Next**.
- e. In the Circuit **Source** dialog box, fill in the source **Node, Slot, Port, and Type** where the test set is connected and click **Next**.
- f. In the Circuit **Destination** dialog box, fill in the destination **Node, Slot, Port, and Type** (the OC-N port in the destination node) and click **Finish**.

**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:
  - From the **View** menu, choose **Go To Other Node**.
  - Choose the node from the drop-down list in the Select Node dialog box and click **OK**.
- b. In node view, double-click the 15310-CL-CTX card with the OC-N port that requires the loopback, such as the 15310-CL-CTX in the destination-node ONS 15310-CL.
- c. Click the **Maintenance > Loopback** tabs.
- d. Select **OOS,MT** from the Admin State column.
- e. Select **Terminal (Inward)** from the Loopback Type column.
- f. Click **Apply**.
- g. Click **Yes** in the confirmation dialog box.

**Step 5** Continue with the “Test the Terminal Loopback Circuit” procedure on page 1-23.

**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 port 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,AINS; OOS,DSBLD; or OOS,MT) in the Admin State column for the port being tested.
• Click **Apply**.
• Click **Yes** in the confirmation dialog box.

b. Clear the terminal loopback circuit:
• Click the **Circuits** tab.
• Choose the loopback circuit being tested.
• Click **Delete**.
• Click **Yes** 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.

---

### 1.4 Restore the Database and Default Settings

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

#### 1.4.1 Restore the Node Database

**Symptom**  One or more nodes are not functioning properly or have incorrect data.  
Table 1-1 describes the potential cause of the symptom and the solution.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect or corrupted node database.</td>
<td>Complete the “Restore the Database” procedure on page 1-24.</td>
</tr>
</tbody>
</table>

**Restore the Database**

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

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

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

a. On the PC connected to the ONS 15310-CL, start Netscape or Internet Explorer.
b. In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15310-CL IP address. A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to an ONS 15310-CL, this process can take several minutes. After the download, the CTC Login dialog box appears.

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

Step 2  In node view, click the Maintenance > Database tabs.
Step 3  Click Restore.
Step 4  Locate the database file stored on the workstation hard drive or on network storage.

Note To clear all existing provisioning, locate and upload the database found on the latest ONS 15310-CL software CD.

Step 5  Click the database file to highlight it.
Step 6  Click Open. The DB Restore dialog box appears. Opening a restore file from another node or from an earlier backup may affect traffic on the login node.
Step 7  Click Yes.
The Restore Database dialog box monitors the file transfer.
Step 8  Wait for the file to complete the transfer to the port.
Step 9  Click OK when the “Lost connection to node, changing to Network View” dialog box appears. Wait for the node to reconnect.

1.4.2 Restore the Node to Factory Configuration

**Symptom**  You are unable reset the ports to make the node functional.

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

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of both ports in the node.</td>
<td>To restore the node to factory configuration, complete the “Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)” procedure on page 1-26 or the “Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)” procedure on page 1-28.</td>
</tr>
<tr>
<td>Replacement of both ports at the same time.</td>
<td>Note  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.</td>
</tr>
</tbody>
</table>

**Table 1-2  Restore the Node to Factory Configuration**
1.4.2 Restore the Node to Factory Configuration

Caution
If you are restoring the database on multiple nodes, wait until the ONS 15310-CL has rebooted on each node before proceeding to the next node.

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

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 use the Search Path field instead of the Package and Database fields. You may 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 1-1 on page 1-27).

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

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

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

Step 1
Insert the ONS 15310-CL System Software CD, Version 5.0.x into the computer CD-ROM drive. If the CTC Installation Wizard appears, click Cancel.

Step 2
From the Windows Start menu, choose Run. In the Run dialog box, click Browse and navigate to the CISCO15310 folder on the software CD.

Step 3
In the Browse dialog box Files of Type field, choose All Files.

Step 4
Choose the RE-INIT.jar file and click Open. The NE Re-Initialization window appears (Figure 1-1).
Step 5  Complete the following fields:

- **GNE IP**—If the node you are reinitializing is accessed through another node configured as a gateway network element (GNE), enter the GNE IP address. If you have a direct connection to the node, leave this field blank.

- **Node IP**—Enter the node name or IP address of the node that you are reinitializing.

- **User ID**—Enter the user ID needed to access the node.

- **Password**—Enter the password for the user ID.

- **Upload Package**—Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.

- **Force Upload**—Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.

- **Activate/Revert**—Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tabs.

- **Re-init Database**—Check this box to send a new database to the node. (This is equivalent to the CTC database restore operation.) If unchecked, the node database is not modified.

- **Confirm**—Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.

- **Search Path**—Enter the path to the CISCO15310 folder on the CD drive.

Step 6  Click **Go**.

Caution  Before continuing with the next step, verify that the database to upload is correct. You cannot reverse the upload process after you click Yes.

Step 7  Review the information on the Confirm NE Re-Initialization dialog box, then click **Yes** to start the reinitialization.

The reinitialization begins. After the software is downloaded and activated, and the database is uploaded to the 15310-CL-CTX card, “Complete” appears in the status bar and the 15310-CL-CTX will reboot. Wait a few minutes for the reboot to complete.

Step 8  After the reboot is complete, log into the node.
Step 9  Manually set the node name and network configuration to site-specific values. See the Cisco ONS 15310-CL Procedure Guide for information about setting the node name, IP address, mask and gateway, and IIOP port.

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

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

⚠️ Caution  Restoring a node to factory configuration on a UNIX workstation should only be carried out on an OOS,MA port.

👉 Note  The ONS 15310-CL reboots several times during this procedure. Wait until it is completely rebooted before continuing.

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

Step 1  Insert the system software CD into the computer CD-ROM drive. If the CTC Installation Wizard appears, click Cancel.

Step 2  To find the recovery tool file, go to the CISCO15310 directory on the CD (usually /cdrom/cdrom0/CISCO15310).

Step 3  If you are using a file explorer, double-click the RE-INIT.jar file. If you are working with a command line, run java -jar RE-INIT.jar. The NE Re-Initialization window appears (Figure 1-1 on page 1-27).

Step 4  Complete the following fields:

- GNE IP—If the node you are reinitializing is accessed through another node configured as a gateway network element (GNE), enter the GNE IP address. If you have a direct connection to the node, leave this field blank.
- Node IP—Enter the node name or IP address of the node that you are reinitializing.
- User ID—Enter the user ID needed to access the node.
- Password—Enter the password for the user ID.
- Upload Package—Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
- Force Upload—Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
- Activate/Revert—Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tabs.
1.5 PC Connectivity Troubleshooting

This section contains troubleshooting procedures for PC and network connectivity to the ONS 15310-CL.

1.5.1 Unable to Verify the IP Configuration of Your PC

**Symptom** When connecting your PC to the ONS 15310-CL, you are unable to successfully ping the IP address of your PC to verify the IP configuration.

Table 1-3 describes the potential causes of the symptom and the solutions.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address is typed incorrectly.</td>
<td>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.</td>
</tr>
<tr>
<td>The IP configuration of your PC is not properly set.</td>
<td>Verify the IP configuration of your PC, see the “Verify the IP Configuration of Your PC” procedure on page 1-30. If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC.</td>
</tr>
</tbody>
</table>
Verify the IP Configuration of Your PC

**Step 1** Open a DOS command window by selecting **Start > Run** from the Start menu.

**Step 2** In the Open field, type **command** and then click **OK**. The DOS command window appears.

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

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

The Windows IP configuration information appears, 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.

**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 causes of the symptom and the solutions.

**Table 1-4 Browser Login Does Not Launch Java**

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The PC operating system and browser are not properly configured.</td>
<td>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 1-30 and the “Reconfigure the Browser” procedure on page 1-31.</td>
</tr>
</tbody>
</table>

**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 15310-CL software CD.

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

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

d. Follow the JRE installation wizard steps.
Step 3  From the Windows start menu, click **Settings > Control Panel**.

Step 4  In the Java Plug-in Control Panel window, double-click the **Java Plug-in 1.4.2** icon.

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

Step 6  From the Java Run Time Environment menu, select **JRE 1.4 in C:\ProgramFiles\JavaSoft\JRE\1.4.2**.

Step 7  Click **Apply**.

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

---

**Reconfigure the Browser**

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

Step 2  If you are using Netscape Navigator:

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

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

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

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

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

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

      - For Windows 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 **OK**.

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

Step 3  If you are using Internet Explorer:

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

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

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

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

Step 4  Temporarily disable any virus-scanning software on the computer. See the “1.6.3 Browser Stalls When Downloading CTC JAR Files from port” section on page 1-36.

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 15310-CL.

Step 7  After completing browser configuration, enable the virus-scanning software on the computer.
Chapter 1 General Troubleshooting

1.5.3 Unable to Verify the NIC Connection on Your PC

**Symptom** When connecting your PC to the ONS 15310-CL, you are unable to verify that the network interface card (NIC) connection is working properly because the link LED is not on or flashing.

Table 1-5 describes the potential causes of the symptom and the solutions.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Category 5 cable is not plugged in properly.</td>
<td>Confirm that both ends of the cable are properly inserted. If the cable is not fully inserted due to a broken locking clip, the cable should be replaced.</td>
</tr>
<tr>
<td>The Category 5 cable is damaged.</td>
<td>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.</td>
</tr>
<tr>
<td>Incorrect type of Category 5 cable is being used.</td>
<td>If you are connecting an ONS 15310-CL directly to your laptop/PC or a router, use a straight-through Category 5 cable. When connecting the ONS 15310-CL 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” procedure on page 1-52.</td>
</tr>
<tr>
<td>The NIC is improperly inserted or installed.</td>
<td>If you are using a Personal Computer Memory Card International Association (PCMCIA)-based NIC, remove and reinsert the NIC to make sure the NIC is fully inserted. If the NIC is built into the laptop/PC, verify that the NIC is not faulty.</td>
</tr>
<tr>
<td>The NIC is faulty.</td>
<td>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.</td>
</tr>
</tbody>
</table>

1.5.4 Verify PC Connection to the ONS 15310-CL (Ping)

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

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

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A lost connection between the PC and the ONS 15310-CL.</td>
<td>Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15310-CL port. A ping command works if the PC connects directly to the port or uses a LAN to access the port. See the “Ping the ONS 15310-CL” procedure on page 1-33.</td>
</tr>
</tbody>
</table>
Ping the ONS 15310-CL

**Step 1**  
Open the command prompt:  
- 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**.  
- 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:  
```markdown
ping ONS-15310-IP-address
```

For example:
```markdown
ping 192.1.0.2
```

**Step 3**  
If the workstation has connectivity to the ONS 15310-CL, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a “Request timed out” message appears.

**Step 4**  
If the ping is successful, an active TCP/IP connection exists. Restart CTC.

**Step 5**  
If the ping is not successful and the workstation connects to the ONS 15310-CL through a LAN, check that the workstation’s IP address is on the same subnet as the ONS 15310-CL.

**Step 6**  
If the ping is not successful and the workstation connects directly to the ONS 15310-CL, check that the link light on the workstation’s NIC is on.

### 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 1-7** describes the potential cause of the symptom and the solution.
1.6.2 Unable to Change Node View to Network View

Symptom: Logging into CTC session, 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 1-8 describes the potential cause of the symptom and the solution.
Chapter 1  General Troubleshooting

1.6.2 Unable to Change Node View to Network View

Table 1-8  Unable to Change Node View to Network View

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The display requires more memory for the graphical user interface (GUI) environment variables.</td>
<td>Set the system or user CTC HEAP environment variable to increase the memory limits.</td>
</tr>
<tr>
<td></td>
<td>See the “Set the CTC HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows” procedure on page 1-35 or the “Set the CTC HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris” procedure on page 1-35 to enable the CTC HEAP variable change.</td>
</tr>
</tbody>
</table>

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

Set the CTC HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows

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

Step 1  Close all open CTC sessions and browser windows.
Step 2  From the Windows Start menu, choose Control Panel > System.
Step 3  In the System Properties window, click the Advanced tab.
Step 4  Click the Environment Variables button to open the Environment Variables window.
Step 5  Click the New button under the System variables field.
Step 6  Type CTC_HEAP in the Variable Name field.
Step 7  Type 512 in the Variable Value field, and then click the OK button to create the variable.
Step 8  Again, click the New button under the System variables field.
Step 9  Type CTC_MAX_PERM_SIZE_HEAP in the Variable Name field.
Step 10  Type 128 in the Variable Value field, and then click the OK button to create the variable.
Step 11  Click the OK button in the Environment Variables window to accept the changes.
Step 12  Click the OK button in the System Properties window to accept the changes.

Set the CTC HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris

Step 1  From the user shell window, kill any CTC sessions and browser applications.
Step 2  In the user shell window, set the environment variables to increase the heap size.

Example

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

```
% setenv CTC_HEAP 512
```
1.6.3 Browser Stalls When Downloading CTC JAR Files from port

Symptom  The browser stalls or hangs when downloading a CTC Java archive (JAR) file from the port. 

Table 1-9 describes the potential cause of the symptom and the solution.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee VirusScan software might be interfering with the operation. The problem</td>
<td>Disable the VirusScan Download Scan feature. See the “Disable the VirusScan Download Scan” procedure on page 1-36.</td>
</tr>
<tr>
<td>occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or</td>
<td></td>
</tr>
<tr>
<td>later.</td>
<td></td>
</tr>
</tbody>
</table>

Comments

- `setenv CTC_MAX_PERM_SIZE_HEAP 128`

1.6.4 CTC Does Not Launch

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

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

Disable the VirusScan Download Scan

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

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

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

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The CTC cache file might be corrupted or might need to be replaced.</td>
<td>Delete the CTC cache file. This operation forces the ONS 15310-CL to download a new set of JAR files to your computer hard drive. See the “Delete the CTC Cache File Automatically” procedure on page 1-38 if you want to temporarily delete the cache stored from another CTC session, or the “Delete the CTC Cache File Manually” procedure on page 1-38 if you want to delete the .jar files associated with an older JRE version.</td>
</tr>
<tr>
<td>Insufficient heap memory allocation.</td>
<td>Increase the heap size if you are using CTC to manage more than 50 nodes concurrently. See the “Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows” procedure on page 1-35 or the “Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris” procedure on page 1-35.</td>
</tr>
</tbody>
</table>

**Note** To avoid network performance issues, Cisco recommends managing a maximum of 50 nodes concurrently with CTC. To manage more than 50 nodes, Cisco recommends using Cisco Transport Manager (CTM). Cisco does not recommend running multiple CTC sessions when managing two or more large networks.
Delete the CTC Cache File Automatically

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

**Step 1**
Enter an ONS 15310-CL 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 **Delete CTC Cache** on the initial browser window to clear the CTC cache. Figure 1-2 shows the Delete CTC Cache window.

Figure 1-2  Deleting the CTC Cache

---

Delete the CTC Cache File Manually

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

**Step 1**
To delete the JAR files manually, from the Windows Start menu choose **Search > For Files or Folders**.
**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 1-12 describes the potential causes of the symptom and the solutions.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Different CTC releases are not recognizing each other. Usually accompanied by an INCOMPATIBLE-SW alarm.</td>
<td>Correct the core version build as described in the “1.6.8 Different CTC Releases Do Not Recognize Each Other” section on page 1-40.</td>
</tr>
<tr>
<td>A username/password mismatch. Usually accompanied by a NOT-AUTHENTICATED alarm.</td>
<td>Correct the username and password as described in the “1.6.9 Username or Password Does Not Match the Port Information” section on page 1-41.</td>
</tr>
<tr>
<td>No IP connectivity between nodes. Usually accompanied by Ethernet-specific alarms.</td>
<td>Verify the Ethernet connections as described in the <em>Cisco ONS 15310-CL Reference Manual</em> Chapter 8, “CTC Network Connectivity.”</td>
</tr>
<tr>
<td>A lost DCC connection. Usually accompanied by a procedural error mismatch (EOC) alarm.</td>
<td>Clear the EOC alarm and verify the DCC connection as described in the “EOC” alarm on page 2-42.</td>
</tr>
</tbody>
</table>

**1.6.7 Java Runtime Environment Incompatible**

**Symptom** The CTC application does not run properly.

Table 1-13 describes the potential cause of the symptom and the solution.
Table 1-13  Java Runtime Environment Incompatible

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The compatible Java 2 JRE is not installed.</td>
<td>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.</td>
</tr>
</tbody>
</table>

Note  The ONS 15310-CL 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 15310-CL software CD and on the Cisco ONS 15310-CL documentation CD. See the “Launch CTC to Correct the Core Version Build” procedure on page 1-40.

Note  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 1-14 on page 1-41.

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

Launch CTC to Correct the Core Version Build

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

**Step 2**  Start the browser.

**Step 3**  Type the ONS 15310-CL IP address of the node that reported the alarm. This can be the original IP address you logged in with or an IP address other than the original.

**Step 4**  Log into CTC. The browser downloads the JAR file from CTC.

1.6.8  Different CTC Releases Do Not Recognize Each Other

**Symptom**  Different CTC releases on the same network do not recognize each other.

Table 1-14 describes the potential cause of the symptom and the solution.
1.6.9 Username or Password Does Not Match the Port Information

**Symptom**  A mismatch often occurs concurrently with a NOT-AUTHENTICATED alarm. Table 1-15 describes the potential causes of the symptom and the solutions.

**Table 1-15  Username or Password Does Not Match the Port Information**

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The username or password entered does not match the information stored in the port.</td>
<td>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 15310-CL, type the CISCO15 username in capital letters and type otbu+1 in lower-case letters. Click <strong>Login</strong>. (In Release 5.0, a password is required.) See the “Verify Correct Username and Password” procedure on page 1-42.</td>
</tr>
</tbody>
</table>
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  Contact the Cisco TAC at http://www.cisco.com/tac or 1-800-553-2447 to have them enter your system and create a new user name and password.

1.6.10 Superuser Password Needs to Be Reset

Symptom  The Superuser password has been lost or compromised.

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

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A security breach or record-keeping error has occurred.</td>
<td>Reset the ONS 15310-CL to the default Superuser UID and password combination using the lamp test button.</td>
</tr>
</tbody>
</table>

Reset the ONS 15310-CL Password

Note  To complete this procedure, you must be on site and have IP connectivity to the node.

Step 1  At the ONS 15310-CL shelf, locate the recessed button labeled LAMP TEST on the front of the unit.

Step 2  Using a pen tip or something of similar size, press in and hold down the recessed button labelled LAMP TEST for five seconds.

Step 3  Release the LAMP TEST button for approximately two seconds.

Step 4  Again press in and hold down the recessed button labelled LAMP TEST for five seconds.

Step 5  Again release the LAMP TEST button.

Step 6  Start a normal CTC session. At the login screen, CTC accepts the default username and password set when the ONS 15310-CL node shipped. The default username is CISCO15 and the password is otbu+1. CISCO15 has Superuser rights and privileges, which allow you to create a user name and assign a password.

Note  Other existing usernames and passwords are not affected by the reset. The superuser reset applies only to the local node where the procedure is performed.

Step 7  If you need to create another user name and password, complete the following steps:

a.  Click the Provisioning > Security tabs and click Create.
b. Fill in the fields with a new user name and password and assign a security level.
c. Click OK.

Note
After new user names and passwords are set up, including at least one Superuser, log in as a newly created Superuser and delete the default CISCO15 username and otbu+1 password to ensure security is not compromised.

1.6.11 No IP Connectivity Exists Between Nodes

Symptom The nodes have a gray icon that is usually accompanied by alarms. Table 1-17 describes the potential cause of the symptom and the solution.

Table 1-17 No IP Connectivity Exists Between Nodes

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost Ethernet connection</td>
<td>Usually, this condition is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in Chapter 8, “CTC Network Connectivity,” of the Cisco ONS 15310-CL Reference Manual.</td>
</tr>
</tbody>
</table>

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

Table 1-18 DCC Connection Lost

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A lost DCC connection</td>
<td>Usually, this condition is accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the “EOC” alarm on page 2-42.</td>
</tr>
</tbody>
</table>

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 1-19 describes the potential cause of the symptom and the solution.
Cancel the Circuit Creation and Start Over

**Step 1** Cancel the circuit creation:
- Click **Cancel**.
- Click **Back** 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 15310-CL.

Table 1-20 describes the potential causes of the symptom and the solutions.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>

### 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 Status

**Symptom** An automatic or manual transition of another state results in the OOS-PARTIAL state; at least one of the connections in the circuit is in IS-NR state and at least one other connection in the circuit is in IS,AINS, OOS,MT, or OOS_AINS state.

Table 1-21 describes the potential causes of the symptom and the solutions.

#### Table 1-21 Circuit in Partial Status

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>During a manual transition, CTC cannot communicate with one of the nodes or one of</td>
<td>Repeat the manual transition operation. If the Partial status persists, determine which node in the circuit is not changing to the desired state. See the “View the State of Circuit Nodes” procedure on page 1-45. Log onto the circuit node that did not change to the desired state and determine the version of software. Refer to the release-specific software upgrade guide for software upgrade procedures.</td>
</tr>
<tr>
<td>the nodes is on a version of software that does not support the new state model.</td>
<td></td>
</tr>
<tr>
<td>During an automatic transition, some path-level defects and/or alarms were</td>
<td>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 1-45. 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 15310-CL Procedure Guide for procedures to clear alarms and change circuit configuration settings. Resolve and clear the defects and alarms on the circuit node and verify that the circuit transitions to the desired state.</td>
</tr>
<tr>
<td>detected on the circuit.</td>
<td></td>
</tr>
<tr>
<td>One end of the circuit is not properly terminated.</td>
<td></td>
</tr>
</tbody>
</table>

#### View the State of Circuit Nodes

- **Step 1** Click the **Circuits** tab.
- **Step 2** From the Circuits tab list, select the circuit with the OOS-PARTIAL status condition.
- **Step 3** Click **Edit**. 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 Circuits Remain in PARTIAL Status

**Symptom** Circuits remain in the PARTIAL status.

Table 1-32 describes the potential cause of the symptom and the solution.
1.7.3 AIS-V on Unused 15310-CL-CTX VT Circuits

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

Table 1-23 describes the potential cause of the symptom and the solution.

### Table 1-23  AIS-V on Unused 15310-CL-CTX VT Circuits

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>An AIS-V indicates that an upstream failure occurred at the virtual tributary (VT) layer. AIS-V alarms also occur on VT circuits that are not carrying traffic and on stranded bandwidth. Perform the “Clear AIS-V on Unused 15310-CL-CTX VT Circuits” procedure on page 1-46.</td>
</tr>
</tbody>
</table>

**Clear AIS-V on Unused 15310-CL-CTX VT Circuits**

1. **Step 1** Determine the affected port.
2. **Step 2** Record the node ID, slot number, port number, and VT number.
3. **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.
4. **Step 4** Uncheck the bidirectional check box in the circuit creation window.
5. **Step 5** Give the unidirectional VT circuit an easily recognizable name, such as DeleteMe.
6. **Step 6** Display the 15310-CL-CTX card in CTC card view. Click the Maintenance > DS1 tabs.
7. **Step 7** Locate the VT that is reporting the alarm (for example, DS3 #2, DS1 #13).
8. **Step 8** From the Loopback Type list, choose Facility (line) and click **Apply**.
9. **Step 9** Click **Circuits**.
10. **Step 10** Find the one-way circuit you created in **Step 3**. Select the circuit and click **Delete**.
11. **Step 11** Click **Yes** in the Delete Confirmation dialog box.
12. **Step 12** In node view, double-click the 15310-CL-CTX card. Card view opens.
13. **Step 13** Click the Maintenance > DS1 tabs.
14. **Step 14** Locate the VT in Facility (line) Loopback list.
15. **Step 15** From the Loopback Type list, choose **None** and then click **Apply**.
1.7.4 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 1-24 describes the potential causes of the symptom and the solutions.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You might have run out of bandwidth on the VT cross-connect matrix at the ONS 15310-CL indicated in the error message.</td>
<td>The matrix has a maximum capacity of 336 bidirectional VT1.5 cross-connects.</td>
</tr>
</tbody>
</table>

1.7.5 OC-3 and DCC Limitations

**Symptom**  There are limitations to OC-3 and DCC usage. Table 1-25 describes the potential cause of the symptom and the solution.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>OC-3 and DCC have limitations for the ONS 15310-CL.</td>
<td>For an explanation of OC-3 and DCC limitations, refer to the DCC Tunnels section of the Cisco ONS 15310-CL Procedure Guide.</td>
</tr>
</tbody>
</table>

1.7.6 ONS 15310-CL Switches Timing Reference

**Symptom**  Timing references switch when one or more problems occur. Table 1-26 describes the potential causes of the symptom and the solutions.
1.7.7 Holdover Synchronization Alarm

**Symptom** The clock is running at a different frequency than normal and the holdover synchronization (HLDOVRSYNC) alarm appears.

Table 1-27 describes the potential cause of the symptom and the solution.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The last reference input has failed.</td>
<td>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 “HLDOVRSYNC” alarm on page 2-60 for a detailed description of this alarm.</td>
</tr>
<tr>
<td>Note</td>
<td>The ONS 15310-CL supports holdover timing per Telcordia GR-4436 when provisioned for external (BITS) timing.</td>
</tr>
</tbody>
</table>

1.7.8 Free-Running Synchronization Mode

**Symptom** The clock is running at a different frequency than normal and the free-running synchronization (FRNGSYNC) alarm appears.

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

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No reliable reference input is available.</td>
<td>The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the “FRNGSYNC” alarm on page 2-57 for a detailed description of this alarm.</td>
</tr>
</tbody>
</table>
1.7.9 Daisy-Chained BITS Not Functioning

**Symptom** You are unable to daisy-chain the BITS.

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

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daisy-chaining BITS is not supported on the ONS 15310-CL.</td>
<td>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 15310-CL.</td>
</tr>
</tbody>
</table>

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 1-30 describes the potential cause of the symptom and the solution.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The card cannot boot because it failed the Power On Shelf Test (POST) diagnostics.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 1-31 describes the potential cause of the symptom and the solution.
### Table 1-31 Bit Errors Appear for a Line Card

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faulty cabling or low</td>
<td>Troubleshoot cabling problems using the “1.1 Network Troubleshooting Tests” section on page 1-2.</td>
</tr>
<tr>
<td>optical-line levels.</td>
<td>Troubleshoot low optical levels using procedures in the “1.8.2 Faulty Fiber-Optic Connections” section on page 1-50.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Bit errors on line (traffic) ports usually originate from cabling problems or low optical-line levels.</td>
</tr>
<tr>
<td></td>
<td>The errors can be caused by synchronization problems, especially if PJ (pointer justification) errors are reported.</td>
</tr>
<tr>
<td></td>
<td>Use a test set whenever possible because the cause of the errors could be external cabling, fiber, or external equipment connecting to the ONS 15310-CL.</td>
</tr>
</tbody>
</table>

### 1.8.2 Faulty Fiber-Optic Connections

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

Table 1-32 describes the potential causes of the symptom and the solutions.

### Table 1-32 Faulty Fiber-Optic Connections

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faulty fiber-optic connections.</td>
<td>Faulty fiber-optic connections can be the source of SONET alarms and signal errors. See the “Verify Fiber-Optic Connections” procedure on page 1-51.</td>
</tr>
<tr>
<td>Faulty Category-5 cables.</td>
<td>Faulty Category-5 cables can be the source of SONET alarms and signal errors. See the “1.8.2.1 Crimp Replacement LAN Cables” procedure on page 1-52.</td>
</tr>
</tbody>
</table>

---

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

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

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

**Step 1** Ensure that a single-mode fiber connects to the ONS 15310-CL small form-factor pluggable (SFP). SM or SM Fiber should be printed on the fiber span cable. ONS 15310-CL ports 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 port being tested (either 1310 nm or 1550 nm).

e. Verify that the power level falls within the range specified for the card; refer to the Cisco ONS 15310-CL Reference Manual for information.

**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 15310-CL Procedure Guide. If possible, do this for the OC-N port you are working on and the far-end ONS 15310-CL.

b. Clean the optical connectors on the port. Clean the connectors according to site practice or, if none exists, follow the procedure in the Cisco ONS 15310-CL Procedure Guide. If possible, do this for the card you are working on and the far-end ONS 15310-CL.

c. 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 port failed. Complete the following steps:

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 15310-CL Procedure Guide. If possible, do this for the card you are working on and the far-end card.

c. Retest the fiber power level.
1.8.2 Faulty Fiber-Optic Connections

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 15310-CL. Use #22 or #24 AWG shielded wire with RJ-45 connectors and a crimping tool.

Use a cross-over cable when connecting an ONS 15310-CL to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15310-CL to a router or workstation.

Figure 1-3 shows the layout of an RJ-45 connector.

![Figure 1-3 RJ-45 Pin Numbers](image)

End view of RJ-45 plug  Looking into an RJ-45 jack

Figure 1-4 shows the layout of a LAN cable.

![Figure 1-4 LAN Cable Layout](image)

Table 1-33 shows LAN cable pinouts.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Color</th>
<th>Pair</th>
<th>Name</th>
<th>Pin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>White/orange</td>
<td>2</td>
<td>Transmit Data +</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Orange</td>
<td>2</td>
<td>Transmit Data -</td>
<td>2</td>
</tr>
</tbody>
</table>
### Table 1-33  LAN Cable Pinout (continued)

<table>
<thead>
<tr>
<th>Pin</th>
<th>Color</th>
<th>Pair</th>
<th>Name</th>
<th>Pin</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>White/green</td>
<td>3</td>
<td>Receive Data +</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td>1</td>
<td>—</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>White/blue</td>
<td>1</td>
<td>—</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td>3</td>
<td>Receive Data –</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>White/brown</td>
<td>4</td>
<td>—</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td>4</td>
<td>—</td>
<td>8</td>
</tr>
</tbody>
</table>

---

### Table 1-34  Cross-Over Cable Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Color</th>
<th>Pair</th>
<th>Name</th>
<th>Pin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>White/orange</td>
<td>2</td>
<td>Transmit Data +</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Orange</td>
<td>2</td>
<td>Transmit Data –</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>White/green</td>
<td>3</td>
<td>Receive Data +</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td>1</td>
<td>—</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>White/blue</td>
<td>1</td>
<td>—</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td>3</td>
<td>Receive Data –</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>White/brown</td>
<td>4</td>
<td>—</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td>4</td>
<td>—</td>
<td>8</td>
</tr>
</tbody>
</table>

---

**Note**

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

Figure 1-5 shows the layout of a cross-over cable.

Figure 1-5  Cross-Over Cable Layout
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 1-35 describes the potential causes of the symptom and the solutions.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of power or low voltage</td>
<td>See Chapter 2, “Alarm Troubleshooting,” for information about specific power alarms. Procedures for installing power supply and cables are located in the Cisco ONS 15310-CL Procedure Guide Chapter 1, “Install Hardware.” Power supplies may be disconnected by reversing the appropriate procedure (for AC or DC power).</td>
</tr>
<tr>
<td>Improperly connected power supply</td>
<td>Note The ONS 15310-CL requires a constant source of DC power to properly function. Input power is –48 VDC. Power requirements range from –42 VDC to –57 VDC. Note A newly installed ONS 15310-CL that is not properly connected to its power supply does not operate. Power problems can be confined to a specific ONS 15310-CL 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 15310-CL to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the Provisioning &gt; General tabs and change the Date and Time fields.</td>
</tr>
</tbody>
</table>

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

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

⚠️ Caution Operations that interrupt power supply or short the power connections to the ONS 15310-CL are service-affecting.
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 1-36 describes the potential cause of the symptom and the solution.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improper power supply.</td>
<td>Refer to power information in the <em>Cisco ONS 15310-CL Procedure Guide</em> Chapter 1, “Install Hardware.”</td>
</tr>
</tbody>
</table>

1.9.3 Lamp Tests for Card LEDs

The LED lamp test determines whether card-level LEDs are operational. For optical and electrical ports, this test also causes port-level LEDs to turn on. For Ethernet cards, only card-level LEDs light. For these cards, port-level LEDs can be compared to the given guidelines to determine whether they are working correctly.

Symptom: Optical (OC-N) or electrical (DS-N) ports LEDs do not light, or you are unsure whether the LEDs are working properly.

Optical and electrical port LEDs light during the lamp test. Ethernet cards only illuminate card-level LEDs during the test. Table 1-37 describes the possible problem and the solution for optical and electrical cards.

<table>
<thead>
<tr>
<th>Possible Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faulty optical and electrical port LED</td>
<td>A lamp test verifies that all the port LEDs work. Run this diagnostic test as part of the initial ONS 15310-CL turn-up, a periodic maintenance routine, or any time you question whether an LED is in working order. Complete the “Verify Card LED Operation” procedure on page 1-55.</td>
</tr>
</tbody>
</table>

Verify Card LED Operation

**Step 1** In CTC, click the **Maintenance > Diagnostic** tabs.

**Step 2** Click **Lamp Test**.

**Step 3** Watch to make sure all the port LEDs illuminate as previously noted for several seconds.

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

With the exceptions previously described, if an OC-N or DS-N LED does not light up, the LED is faulty. Return the defective card to Cisco through the RMA process. Contact Cisco TAC at [http://www.cisco.com/tac](http://www.cisco.com/tac) or 1-800-553-2447.
1.9.3 Lamp Tests for Card LEDs