Turn Up Node

This chapter explains how to provision a single Cisco ONS 15454 node and turn it up for service, including node name, date and time, timing references, network attributes such as IP address and default router, users and user security, and card protection groups.

If you are provisioning an ONS 15454 for dense wavelength division multiplexing (DWDM) or as a hybrid node (DWDM and TDM), you will not complete some procedures until directed to do so in Chapter 5, "Turn Up a DWDM Node." These procedures are identified in the procedures list in the following section.

Before You Begin

Complete the procedures applicable to your site plan from the following chapters:

- Chapter 1, "Install the Shelf and Backplane Cable"
- Chapter 2, "Install Cards and Fiber-Optic Cable"
- Chapter 3, "Connect the PC and Log into the GUI"

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A24 Verify Card Installation, page 4-2—Complete this procedure first.
2. NTP-A30 Create Users and Assign Security, page 4-4—Complete this procedure to create Cisco Transport Controller (CTC) users and assign their security levels.
3. NTP-A25 Set Up Name, Date, Time, and Contact Information, page 4-7—Continue with this procedure to set the node name, date, time, location, and contact information.
4. NTP-A261 Set Power Monitor Thresholds, page 4-9—Continue with this procedure to set the node battery power thresholds.
5. NTP-A169 Set Up CTC Network Access, page 4-9—Continue with this procedure to provision the IP address, default router, subnet mask, and network configuration settings.
6. NTP-A27 Set Up the ONS 15454 for Firewall Access, page 4-19—Continue with this procedure if the ONS 15454 will be accessed behind firewalls.
7. NTP-A28 Set Up Timing, page 4-22—Continue with this procedure to set up the node's SONET timing references. If you are turning up a DWDM or hybrid node, do not complete this procedure until directed to do so in Chapter 5, "Turn Up a DWDM Node."

8. NTP-A170 Create Protection Groups, page 4-26—Complete this procedure, as needed, to set up 1:1, 1:N, 1+1, or Y-cable protection groups for ONS 15454 electrical and optical cards. If you are turning up a DWDM or hybrid node, do not complete this procedure until directed to do so in Chapter 5, "Turn Up a DWDM Node."
9. NTP-A256 Set Up SNMP, page 4-33—Complete this procedure if simple network management protocol (SNMP) will be used for network monitoring.

NTP-A24 Verify Card Installation

Purpose	This procedure verifies that an ONS 15454 node provisioned for SONET is ready for turn up.
Tools/Equipment	An engineering work order, site plan, or other document specifying the ONS 15454 card installation.
Prerequisite Procedures	Chapter 1, "Install the Shelf and Backplane Cable" Chapter 2, "Install Cards and Fiber-Optic Cable"
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Verify that two TCC2 cards are installed in Slots 7 and 11.

Step 2 Verify that the green ACT (active) LED is illuminated on one TCC2 and the amber STBY (standby) LED is illuminated on the second TCC2.

Note If the TCC2 cards are not installed, or if their LEDs are not operating as described, do not proceed. Repeat the "DLP-A36 Install the TCC2 Cards" task on page 2-7, or refer to the *Cisco ONS 15454 Troubleshooting Guide* to resolve installation problems before proceeding to Step 3.

If you are provisioning the ONS 15454 for DWDM, continue with Step 17. Otherwise, continue with the next step.

Step 3 Verify that cross-connect cards (XC, XCVT, or XC10G) are installed in Slots 8 and 10. The cross-connect cards must be the same type.

Step 4 Verify that the green ACT (active) LED is illuminated on one cross-connect card and the amber STBY (standby) LED is illuminated on the second cross-connect card.

Note If the cross-connect cards are not installed, or if their LEDs are not operating as described, do not proceed. Repeat the "DLP-A37 Install the XC, XCVT, or XC10G Cards" task on page 2-9, or refer to the *Cisco ONS 15454 Troubleshooting Manual* to resolve installation problems before proceeding to Step 5.

If you are provisioning the ONS 15454 for DWDM and TDM (hybrid node), continue with Step 17. Otherwise, continue with the next step.

Step 5 If your site plan requires an AIC or AIC-I card, verify that the AIC/AIC-I card is installed in Slot 9 and its ACT (active) LED displays a solid green light.

Step 6 Verify that electrical cards (DS-1, DS-3, EC-1, and DS3XM-6) are installed in Slots 1 to 6 or 12 to 17 as designated by your installation plan.

Step 7 If your site plan requires an Ethernet card, verify that the Ethernet card is installed in the specified slot and its ACT (active) LED displays a solid green light:

- The E100T-12, E100T-12-G, E1000-2, and E1000-2-G cards are installed in Slots 1 to 6 or 12 to 17
- The G1000-4 cards are installed in Slots 1 to 4 or 14 to 17.
- The G1K-4, ML1000-2, and ML100T-12 cards can be installed in Slots 1 to 6 or 12 to 17 if an XC10G cross-connect is installed. However, they must be installed in Slots 5, 6, 12, or 13 if XC or XCVT cards are installed.

Step 8 If Ethernet cards are installed, verify that the correct cross-connect cards are installed in Slots 8 and 10:

- E100T-12-G, E1000-2-G, and G1000-4 cards require XC10G cards.
- G1K-4, ML1000-2, and ML100T-12 cards require XC10G cards if they are installed in Slots 1 to 4 or 14 to 17.

Step 9 If an E1000-2, E1000-2-G, G1000-4, or ML1000-2 Ethernet card is installed, verify that it has a gigabit interface converter (GBIC) or SFP installed. If not, see the "DLP-A469 Install GBIC or SFP Connectors" task on page 2-20.

Step 10 Verify that OC-N cards (OC-3, OC-3-8, OC-12, OC-12-4, OC-48, OC-48 any slot [AS], and OC-192) are installed in the slots designated by your site plan.

- OC-3, OC-12, and OC-48 AS cards can be installed in Slots 1 to 6 or 12 to 17.
- OC-3-8 and OC-12-4 can be installed in Slots 1 to 4 and 14 to 17.
- OC-48 and OC-192 can be installed in Slots 5, 6, 12, or 13.

Step 11 Verify that the correct cross-connect cards are installed in Slots 8 and 10:

- If an OC-192, OC-12-4, or OC-3-8 card is installed, an XC10G card must be installed.
- If an OC-48 AS card is installed in Slots 1 to 4 or 14 to 17, an XC10G card must be installed. If XC or XCVT cards are installed, the OC-48 AS can be installed only in Slots 5, 6, 12, or 13.

Step 12 Verify that all installed OC-N cards display a solid amber STBY LED.

Step 13 If transponder or muxponder cards are installed (TXP_MR_10G, MXP_2.5G_10G, TXP_MR_2.5, or TXPP_MR_2.5G), verify that they are installed in Slots 1 to 6 or 12 to 17 and have GBIC or SFP connectors are installed. If GBICs or SFP connectors are not installed, complete the "DLP-A469 Install GBIC or SFP Connectors" task on page 2-20.

Step 14 If Fibre Channel cards (FC-MR-4) are installed, verify one of the following:

- If XC10G cross-connect cards are installed, the FC-MR-4 is installed in Slots 1 to 6 or 12 to 17 and displays a solid green ACT (Active) LED.
- If XCVT cross-connect cards are installed, the FC-MR-4 is installed in Slots 5 to 6 or 12 to 13 and displays a solid green ACT (Active) LED.

Step 15 Verify that fiber-optic cables (fiber) are installed and connected to the locations indicated in the site plan. If the fiber is not installed, complete the "NTP-A247 Install Fiber-Optic Cables on OC-N Cards" procedure on page 2-29.

Step 16 Verify that fiber is routed correctly in the shelf assembly and fiber boots are installed properly. If the fiber is not routed on the shelf assembly, complete the "NTP-A245 Route Fiber-Optic Cables" procedure on page 2-56. If the fiber boots are not installed, complete the "DLP-A45 Install the Fiber Boot" task on page 2-39.

Step 17 Verify that the software release shown on the LCD matches the software release indicated in your site plan. If the release does not match, perform one of the following procedures:

- Perform a software upgrade using a Cisco ONS 15454 software CD. Refer to the *Cisco ONS 15454 Software Upgrade Guide* for instructions.
- Replace the TCC2 cards with cards containing the correct release. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Stop. **You have completed this procedure**.

NTP-A30 Create Users and Assign Security

Purpose	This procedure creates ONS 15454 users and assigns their security levels.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you need to create users. If you are already logged in, continue with Step 2.

Note You must log in as a Superuser to create additional users. The CISCO15 user provided with each ONS 15454 can be used to set up other ONS 15454 users. You can add up to 500 users to one ONS 15454.

Step 2 Complete the "DLP-A74 Create a New User—Single Node" task on page 4-5 or the "DLP-A75 Create a New User—Multiple Nodes" task on page 4-5 as needed.

Note You must add the same user name and password to each node a user will access.

Step 3 If you want to modify the security policy settings, including password aging and idle user timeout policies, complete the "NTP-A205 Modify Users and Change Security" procedure on page 12-25.

Stop. **You have completed this procedure**.

DLP-A74 Create a New User—Single Node

Purpose	This task creates a new user for one ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > Security > Users** tabs.

Step 2 In the Users window, click **Create**.

Step 3 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must be 6 to 10 characters.
- Password—Type the user password. The password must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are nonalphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the *Cisco ONS 15454 Reference Manual* for information about the capabilities provided with each level.

Note Each security level has a different idle time. The idle time is the length of time that CTC can remain idle before the password must be reentered. The defaults are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle times, refer to the "NTP-A205 Modify Users and Change Security" procedure on page 12-25.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A75 Create a New User—Multiple Nodes

Purpose	This task adds a new user to multiple ONS 15454s.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note All nodes where you want to add users must be accessible in network view.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Security > Users** tabs.

Step 3 In the Users window, click **Create**.

Step 4 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must 6 to 10 characters.
- Password—Type the user password. The password must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) and special (+, #, %) characters, where at least two characters are nonalphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the *Cisco ONS 15454 Reference Manual* for information about the capabilities provided with each level.

Note Each security level has a different idle time. The idle time is the length of time that CTC can remain idle before it locks up and the password must be reentered. The defaults are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle times, refer to the "NTP-A205 Modify Users and Change Security" procedure on page 12-25.

Step 5 Under "Select applicable nodes," deselect any nodes where you do not want to add the user (all network nodes are selected by default).

Step 6 Click **OK**.

Step 7 In the User Creation Results dialog box, verify that the user was added to all the nodes chosen in Step 5. If not, click **OK** and repeat Steps 2 through 6. If the user was added to all nodes, click **OK** and continue with the next step.

Step 8 Return to your originating procedure (NTP).

NTP-A25 Set Up Name, Date, Time, and Contact Information

Purpose	This procedure provisions identification information for the node, including the node name, a contact name and phone number, the location of the node, and the date, time, and time zone.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 for the node you will turn up. If you are already logged in, continue with Step 2.

Step 2 Click the **Provisioning > General** tabs.

Step 3 Enter the following information in the fields listed:

- Node Name—Type a name for the node. For TL1 compliance, names must begin with an alpha character and have no more than 20 alphanumeric (a-z, A-Z, 0-9) characters.
- Contact—Type the name of the node contact person and the phone number, up to 255 characters (optional).
- Latitude—Enter the node latitude: N (North) or S (South), degrees, and minutes (optional).
- Longitude—Enter the node longitude: E (East) or W (West), degrees, and minutes (optional).

Tip You can also position nodes manually on the network view map. Press Ctrl while you drag and drop the node icon. To create the same network map visible for all ONS 15454 users, complete the "NTP-A172 Create a Logical Network Map" procedure on page 6-52.

CTC uses the latitude and longitude to position ONS 15454 icons on the network view map. To convert a coordinate in degrees to degrees and minutes, multiply the number after the decimal by 60. For example, the latitude 38.250739 converts to 38 degrees, 15 minutes (0.250739 x 60 = 15.0443, rounded to the nearest whole number).

- Description—Type a description of the node. The description can be a maximum of 255 characters.
- Use NTP/SNTP Server—When checked, CTC uses a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) server to set the date and time of the node.

  If you do not use an SNTP or NTP server, complete the Date and Time fields. The ONS 15454 will use these fields for alarm dates and times. (CTC displays all alarms in the login node's time zone for cross network consistency.)

Note Using an NTP or SNTP server ensures that all ONS 15454 network nodes use the same date and time reference. The server synchronizes the node's time after power outages or software upgrades.

If you check the Use NTP/SNTP Server check box, type the IP address of one of the following:

  - an NTP/SNTP server connected to the ONS 15454

– Another ONS 15454 with NTP/SNTP enabled that is connected to the ONS 15454

If you check gateway network element (GNE) for the ONS 15454 proxy server (see "DLP-A249 Provision IP Settings" task on page 4-10), external ONS 15454s must reference the gateway ONS 15454 for NTP/SNTP timing. For more information about the ONS 15454 gateway settings, refer to the *Cisco ONS 15454 Reference Manual*.

Caution If you reference another ONS 15454 for the NTP/SNTP server, make sure the second ONS 15454 references an NTP/SNTP server and not the first ONS 15454 (that is, do not create an NTP/SNTP timing loop by having two ONS 15454s reference each other).

- Date—If Use NTP/SNTP Server is not checked, type the current date in the format mm/dd/yyyy, for example, September 24, 2002 is 09/24/2002.
- Time—If Use NTP/SNTP Server is not checked, type the current time in the format hh:mm:ss, for example, 11:24:58. The ONS 15454 uses a 24-hour clock, so 10:00 PM is entered as 22:00:00.
- Time Zone—Click the field and choose a city within your time zone from the drop-down menu. The menu displays the 80 World Time Zones from –11 through 0 (GMT) to +14. Continental United States time zones are GMT-05:00 (Eastern), GMT-06:00 (Central), GMT-07:00 (Mountain), and GMT-08:00 (Pacific).
- Use Daylight Savings Time—Check this check box if the time zone that you chose is using Daylight Savings Time.
- Insert AIS-V on STS-1 SD-P—Check this check box if you want AIS-Vs inserted on VT circuits carried by STS-1s when the STS-1 crosses its SD-P BER threshold. On protected circuits, traffic will be switched. If the switch cannot be performed, or if circuits are not protected, traffic will be dropped when the STS-1 SD-P BER threshold is reached.
- SD-P BER—If you selected Insert AIS-V, you can choose the SD-P BER level from the SD-P BER drop-down menu.

Step 4 Click **Apply**.

Step 5 In the confirmation dialog box, click **Yes**.

Step 6 Review the node information. If you need to make corrections, repeat Steps 3 through 5 to enter the corrections. If the information is correct, continue with the "NTP-A261 Set Power Monitor Thresholds" procedure on page 4-9.

Stop. **You have completed this procedure**.

NTP-A261 Set Power Monitor Thresholds

Purpose	This procedure provisions extreme high, high, extreme low, and low input battery power thresholds within a –48 volts direct current (VDC) environment. When the thresholds are crossed, the TCC2 generates warning alarms in CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 for the node you will set up. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > General > Power Monitor** tabs.

Step 3 To change the extreme low battery voltage threshold in 0.5 VDC increments, choose a voltage from the **ELWBATVGVdc** drop-down menu.

Step 4 To change the low battery voltage threshold in 0.5 VDC increments, choose a voltage from the **LWBATVGVdc** drop-down menu.

Step 5 To change the high battery voltage threshold in 0.5 VDC increments, choose a voltage from the **HIBATVGVdc** drop-down menu.

Step 6 To change the extreme high battery voltage threshold in 0.5 VDC increments, choose a voltage from the **EHIBATVGVdc** drop-down menu.

Step 7 Click **Apply**.

Stop. **You have completed this procedure**.

NTP-A169 Set Up CTC Network Access

Purpose	This procedure provisions network access for a node, including its subnet mask, default router, Dynamic Host Configuration Protocol (DHCP) server, IIOP (Internet Inter-Orb Protocol) listener port, proxy server settings, static routes, Open Shortest Path First (OSPF) protocol, and Routing Information Protocol (RIP).
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A249 Provision IP Settings" task on page 4-10 to provision the ONS 15454 IP address, subnet mask, default router, DHCP server, IIOP listener port, and proxy server settings.

Tip If you cannot log into the node, you can change its IP address, default router, and network mask by using the LCD on the ONS 15454 fan-tray assembly (unless LCD provisioning is suppressed). See the "DLP-A64 Set the IP Address, Default Router, and Network Mask Using the LCD" task on page 4-13 for instructions. However, you cannot use the LCD to provision any other network settings.

Step 3 If static routes are needed, complete the "DLP-A65 Create a Static Route" task on page 4-15. Refer to the *Cisco ONS 15454 Reference Manual* for further information about static routes.

Step 4 If the ONS 15454 is connected to a LAN or WAN that uses OSPF, complete the "DLP-A250 Set Up or Change Open Shortest Path First Protocol" task on page 4-16.

Step 5 If the ONS 15454 is connected to a LAN or WAN that uses RIP, complete the "DLP-A251 Set Up or Change Routing Information Protocol" task on page 4-18.

Stop. **You have completed this procedure**.

DLP-A249 Provision IP Settings

Purpose	This task provisions IP settings, which includes the IP address, default router, DHCP access, firewall access, and proxy server settings for an ONS 15454 node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution All network changes should be approved by your network (or LAN) administrator.

Step 1 In node view, click the **Provisioning** > **Network** tabs.

Step 2 Complete the following information in the fields listed:

- IP Address—Type the IP address assigned to the ONS 15454 node.
- Suppress CTC IP Display—Check this check box if you want to prevent the node IP address from being displayed in CTC to users with Provisioner, Maintenance, or Retrieve security levels. (The IP address suppression is not applied to users with Superuser security level.)
- LCD IP Display—Choose one of the following:
  - Allow Configuration—Displays the node IP address on the LCD and allows users to change the IP settings using the LCD. This option enables the "DLP-A64 Set the IP Address, Default Router, and Network Mask Using the LCD" task on page 4-13.
  - Display Only—Displays the node IP address on the LCD but does not allow users to change the IP address using the LCD.

  - Suppress Display—Suppresses the node IP address display on the LCD.

- Default Router—If the ONS 15454 must communicate with a device on a network that the ONS 15454 is not directly connected to, the ONS 15454 can forward the packets to the default router. Type the IP address of the router in this field.

Note This field is ignored if the node is not connected to a LAN, or if you enable any of the gateway settings to implement the ONS 15454 proxy server feature.

- Forward DHCP Request To—Check this check box to enable DHCP. Also, enter the DHCP server IP address in the Request To field. Unchecked is the default. If you will enable any of the gateway settings to implement the ONS 15454 proxy server features, leave this field blank.

Note If you enable DHCP, computers connected to an ONS 15454 node can obtain temporary IP addresses from an external DHCP server. The ONS 15454 only forwards DHCP requests; it does not act as a DHCP server.

- MAC Address—(*Display only.*) Displays the ONS 15454 IEEE 802 MAC address.
- Net/Subnet Mask Length—Type the subnet mask length (decimal number representing the subnet mask length in bits) or click the arrows to adjust the subnet mask length. The subnet mask length is the same for all ONS 15454s in the same subnet.
- TCC CORBA (IIOP) Listener Port—Provisions the ONS 15454 IIOP listener port. This listener port enables communication with the ONS 15454 through firewalls. See the "NTP-A27 Set Up the ONS 15454 for Firewall Access" procedure on page 4-19 for more information.
- Gateway Settings—Provides options that enable the ONS 15454 proxy server features. Do not select any of these options until you review the proxy server scenario in the *Cisco ONS 15454 Reference Manual*. In proxy server networks, the ONS 15454 is either an external network element (ENE), gateway network element (GNE), or proxy-only server. Provisioning must be consistent for each NE type.
- Enable proxy server on port—If checked, the ONS 15454 serves as a proxy for connections between CTC clients and ONS 15454s that are DCC-connected to the proxy ONS 15454. The CTC client establishes connections to data communications channel (DCC)-connected nodes through the proxy node. The CTC client does not require IP connectivity to the DCC-connected nodes, only to the proxy ONS 15454. If Enable proxy server on port is off, the node does not proxy for any CTC clients, although any established proxy connections continue until the CTC client exits. When this box is checked, you can set the node as an ENE or a GNE:
  - External Network Element (ENE)—If selected, the CTC computer is only visible to the ONS 15454 to which the CTC computer is connected. The computer is not visible to other DCC-connected nodes. In addition, firewall is enabled, which means that the node prevents IP traffic from being routed between the DCC and the LAN port.
  - Gateway Network Element (GNE)—If selected, the CTC computer is visible to other DCC-connected nodes. The node prevents IP traffic from being routed between the DCC and the LAN port.
  - Proxy-only—If selected, the ONS 15454 responds to CTC requests with a list of DCC-connected nodes for which the node serves as a proxy. The CTC computer is visible to other DCC-connected nodes. The node does not prevent traffic from being routed between the DCC and LAN port.

Step 3 Click **Apply**.

Step 4 Click **Yes** in the confirmation dialog box.

Both TCC2 cards reboot, one at a time. During this time (approximately 5 minutes), the active and standby TCC2 card LEDs go through the cycle shown in Table 4-1. Eventually, a "Lost node connection, switching to network view" message appears.

Table 4-1 LED Behavior During TCC2 Reboot

Reboot Activity	Active TCC2 LEDs	Standby TCC2 LEDs
Standby TCC2 card updated with new network information. Memory test (1 to 2 minutes). If an AIC or AIC-I card is installed, AIC FAIL and alarm LEDs light up briefly when the AIC is updated. The standby TCC2 becomes the active TCC2.	ACT/STBY: Flashing green.	1. ACT/STBY: Flashing yellow. 2. FAIL LED: Solid red. 3. All LEDs on except ACT/STBY. 4. CRIT turns off. 5. MAJ and MIN turn off. 6. REM, SYNC, and ACO turn off. 7. All LEDs (except A&B PWR) turn off (1 to 2 minutes). 8. ACT/STBY: Solid yellow. 9. Alarm LEDs: Flash once. 10. ACT/STBY: Solid green.
Memory test (1 to 2 minutes). TCC2 updated with new network information. The active TCC2 becomes the standby TCC2.	1. All LEDs: Turn off (1 to 2 minutes). CTC displays "Lost node connection, switching to network view" message. 2. FAIL LED: Solid red. 3. FAIL LED: Flashing red. 4. All LEDs on except ACT/STBY. 5. CRIT turns off. 6. MAJ and MIN turn off. 7. REM, SYNC, and ACO turn off; all LEDs are off. 8. ACT/STBY: Solid yellow. 9. ACT/STBY: Flashing yellow. 10. ACT/STBY: Solid yellow.	ACT/STBY: Solid green.

Step 5 Click **OK**. The network view appears. The node icon appears in gray, during which time you cannot access the node.

Step 6 Double-click the node icon when it becomes green.

Step 7 Return to your originating procedure (NTP).

DLP-A64 Set the IP Address, Default Router, and Network Mask Using the LCD

Purpose	This task changes the ONS 15454 IP address, default router, and network mask using the LCD on the fan-tray assembly. Use this task if you cannot log into CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A36 Install the TCC2 Cards, page 2-7
Required/As Needed	Optional
Onsite/Remote	Onsite
Security Level	None

Note You cannot perform this task if the LCD IP Display on the node view Provisioning > Network tab is set to Display Only or Suppress Display. See "DLP-A249 Provision IP Settings" task on page 4-10 to view or change the LCD IP Display field.

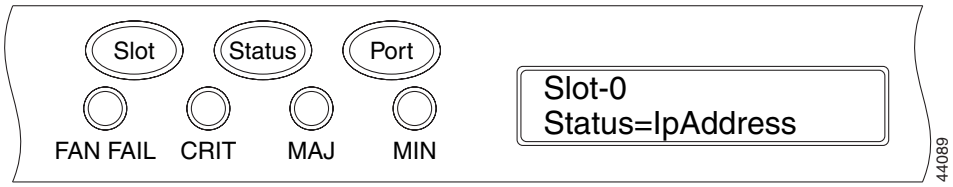
Note The LCD reverts to normal display mode after 5 seconds of button inactivity.

Step 1 On the ONS 15454 front panel, repeatedly press the **Slot** button until Node appears on the LCD.

Step 2 Repeatedly press the **Port** button until the following displays:

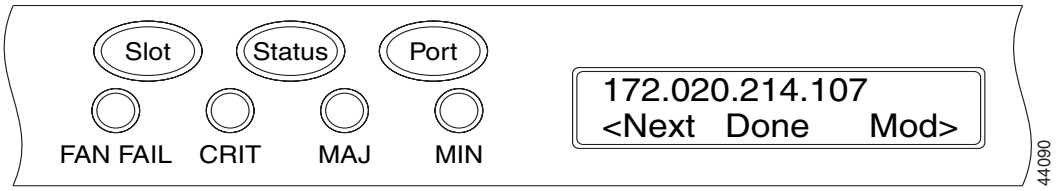
- To change the node IP address, Status=IpAddress (Figure 4-1)
- To change the node network mask, Status=Net Mask
- To change the default router IP address, Status=Default Rtr

Figure 4-1 Selecting the IP Address Option



Step 3 Press the **Status** button to display the node IP address (Figure 4-2), the node subnet mask length, or the default router IP address.

Figure 4-2 Changing the IP Address



Step 4 Push the **Slot** button to move to the IP address or subnet mask digit you need to change. The selected digit flashes.

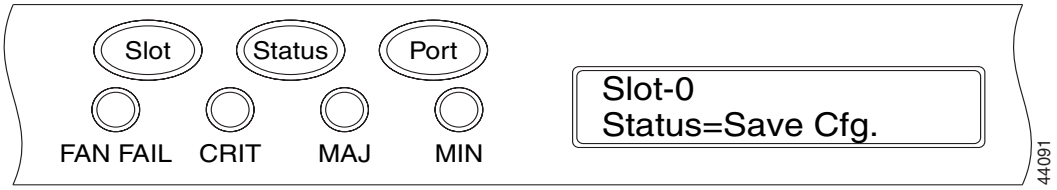
Tip The Slot, Status, and Port button positions correspond to the command position on the LCD. For example, in Figure 4-2, you press the Slot button to invoke the Next command and the Port button to invoke the Done command.

Step 5 Press the **Port** button to cycle the IP address or subnet mask to the correct digit.

Step 6 When the change is complete, press the **Status** button to return to the Node menu.

Step 7 Repeatedly press the **Port** button until the Save Configuration option appears (Figure 4-3).

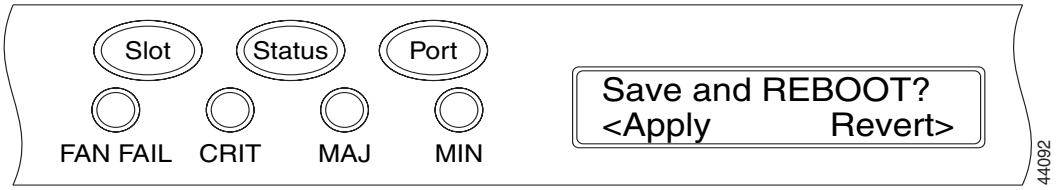
Figure 4-3 Selecting the Save Configuration Option



Step 8 Press the **Status** button to choose the Save Configuration option.

A Save and REBOOT message appears (Figure 4-4).

Figure 4-4 Saving and Rebooting the TCC2



Step 9 Press the **Slot** button to apply the new IP address configuration or press **Port** to cancel the configuration.

Saving the new configuration causes the TCC2 cards to reboot. During the reboot, a "Saving Changes - TCC Reset" message displays on the LCD. The LCD returns to the normal alternating display after the TCC2 reboot is complete (see Table 4-1 on page 4-12 for reboot behavior).

Note The IP address and default router must be on the same subnet. If not, you cannot apply the configuration.

Step 10 Return to your originating procedure (NTP).

DLP-A65 Create a Static Route

Purpose	This task creates a static route to establish CTC connectivity to a computer on another network.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required if either of the following conditions are is true: • CTC computers on one subnet need to connect to ONS 15454s that are connected by a router to ONS 15454s residing on another subnet. OSPF is not enabled and the External Network Element gateway setting is not checked. • You need to enable multiple CTC sessions among ONS 15454s residing on the same subnet and the External Network Element gateway setting is not enabled.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** tabs.

Step 2 Click the **Static Routing** tab. Click **Create**.

Step 3 In the Create Static Route dialog box, enter the following:

- Destination—Enter the IP address of the computer running CTC. To limit access to one computer, enter the full IP address and a subnet mask of 255.255.255.255. To allow access to all computers on the 192.168.1.0 subnet, enter 192.168.1.0 and a subnet mask of 255.255.255.0. You can enter a destination of 0.0.0.0 to allow access to all CTC computers that connect to the router.
- Mask—Enter a subnet mask. If the destination is a host route (that is, one CTC computer), enter a 32-bit subnet mask (255.255.255.255). If the destination is a subnet, adjust the subnet mask accordingly, for example, 255.255.255.0. If the destination is 0.0.0.0, CTC automatically enters a subnet mask of 0.0.0.0 to provide access to all CTC computers. You cannot change this value.
- Next Hop—Enter the IP address of the router port or the node IP address if the CTC computer is connected to the node directly.
- Cost—Enter the number of hops between the ONS 15454 and the computer.

Step 4 Click **OK**. Verify that the static route appears in the Static Route window.

Note Static route networking examples are provided in the IP networking section of the *Cisco ONS 15454 Reference Manual*.

Step 5 Return to your originating procedure (NTP).

DLP-A250 Set Up or Change Open Shortest Path First Protocol

Purpose	This task enables the Open Shortest Path First (OSPF) routing protocol on the ONS 15454. Perform this task if you want to include the ONS 15454 in OSPF-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 You will need the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router to which the ONS 15454 is connected.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Network > OSPF** tabs.

Step 2 On the top left side of the OSPF pane, complete the following:

- DCC/GCC OSPF Area ID Table—In dotted decimal format, enter the number that identifies the ONS 15454s as a unique OSPF area ID. The Area ID can be any number between 000.000.000.000 and 255.255.255.255, but must be unique to the LAN OSPF area.
- SDCC Metric—This value is normally unchanged. It sets a cost for sending packets across the Section DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default SDCC metric is 10. The metric changes to 100 if you check the OSPF Active on LAN check box in Step 3.
- LDCC Metric—Sets a cost for sending packets across the Line DCC. This value should always be lower than the SDCC metric. The default LDCC metric is 33. It is usually not changed.

Step 3 In the OSPF on LAN area, complete the following:

- OSPF active on LAN—When checked, enables the ONS 15454 OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15454s that directly connect to OSPF routers.
- LAN Port Area ID—Enter the OSPF area ID (dotted decimal format) for the router port where the ONS 15454 is connected. (This number is different from the DCC/GCC OSPF Area ID.)

Step 4 By default, OSPF is set to No Authentication. If the OSPF router requires authentication, complete the following steps. If not, continue with Step 5.

a. Click the **No Authentication** button.

b. In the Edit Authentication Key dialog box, complete the following:

- Type—Choose **Simple Password**.
- Enter Authentication Key—Enter the password.
- Confirm Authentication Key—Enter the same password to confirm it.

c. Click **OK**.

The authentication button label changes to Simple Password.

Step 5 Provision the OSPF priority and interval settings.

The OSPF priority and interval defaults are ones most commonly used by OSPF routers. Verify that these defaults match the ones used by the OSPF router where the ONS 15454 is connected.

- Router Priority—Selects the designated router for a subnet.
- Hello Interval (sec)—Sets the number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Dead Interval—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.
- Transit Delay (sec)—Indicates the service speed. One second is the default.
- Retransmit Interval (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- LAN Metric—Sets a cost for sending packets across the LAN. This value should always be lower than the DCC metric. Ten is the default.

Step 6 Under OSPF Area Range Table, create an area range table if one is needed:

Note Area range tables consolidate the information that is outside an OSPF area border. One ONS 15454 in the ONS 15454 OSPF area is connected to the OSPF router. An area range table on this node points the router to the other nodes that reside within the ONS 15454 OSPF area.

a. Under OSPF Area Range Table, click **Create**.

b. In the Create Area Range dialog box, enter the following:

- Range Address—Enter the area IP address for the ONS 15454s that reside within the OSPF area. For example, if the ONS 15454 OSPF area includes nodes with IP addresses 10.10.20.100, 10.10.30.150, 10.10.40.200, and 10.10.50.250, the range address would be 10.10.0.0.
- Range Area ID—Enter the OSPF area ID for the ONS 15454s. This is either the ID in the DCC OSPF Area ID field or the ID in the Area ID for LAN Port field.
- Mask Length—Enter the subnet mask length. In the Range Address example, this is 16.
- Advertise—Check if you want to advertise the OSPF range table.

c. Click **OK**.

Step 7 All OSPF areas must be connected to Area 0. If the ONS 15454 OSPF area is not physically connected to Area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to Area 0:

a. Under OSPF Virtual Link Table, click **Create**.

b. In the Create Virtual Link dialog box, complete the following fields. OSPF settings must match OSPF settings for the ONS 15454 OSPF area:

- Neighbor—The router ID of the Area 0 router.
- Transit Delay (sec)—The service speed. One second is the default.
- Hello Int (sec)—The number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Auth Type—If the router where the ONS 15454 is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
- Retransmit Int (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- Dead Int (sec)—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.

c. Click **OK**.

Step 8 After entering ONS 15454 OSPF area data, click **Apply**.

If you changed the Area ID, the TCC2 cards reset, one at a time. The reset takes approximately 10 to 15 minutes. Table 4-1 on page 4-12 shows the LED behavior during the TCC2 reset.

Step 9 Return to your originating procedure (NTP).

DLP-A251 Set Up or Change Routing Information Protocol

Purpose	This task enables Routing Information Protocol (RIP) on the ONS 15454. Perform this task if you want to include the ONS 15454 in RIP-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 You need to create a static route to the router adjacent to the ONS 15454 for the ONS 15454 to communicate its routing information to non-DCC-connected nodes.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Network > RIP** tabs.

Step 2 Check the **RIP Active** check box if you are activating RIP.

Step 3 Choose either RIP Version 1 or RIP Version 2 from the drop-down menu, depending on which version is supported in your network.

Step 4 Set the RIP metric. The RIP metric can be set to a number between 1 and 15 and represents the number of hops.

Step 5 By default, RIP is set to No Authentication. If the router that the ONS 15454 is connected to requires authentication, complete the following steps. If not, continue with Step 6.

a. Click the **No Authentication** button.

b. In the Edit Authentication Key dialog box, complete the following:

- Type—Choose **Simple Password**.
- Enter Authentication Key—Enter the password,
- Confirm Authentication Key—Enter the same password to confirm it.

c. Click **OK**.

The authentication button label changes to Simple Password.

Step 6 If you want to complete an address summary, complete the following steps. If not, continue with Step 7. Complete the address summary only if the ONS 15454 is a gateway NE with multiple external ONS 15454 NEs attached with IP addresses in different subnets.

a. In the RIP Address Summary area, click **Create**.

b. In the Create Address Summary dialog box, complete the following:

- Summary Address—Enter the summary IP address.

- Mask Length—Enter the subnet mask length using the up and down arrows.
- Hops—Enter the number of hops. The smaller the number of hops, the higher the priority.

c. Click **OK.**

Step 7 Return to your originating procedure (NTP).

NTP-A27 Set Up the ONS 15454 for Firewall Access

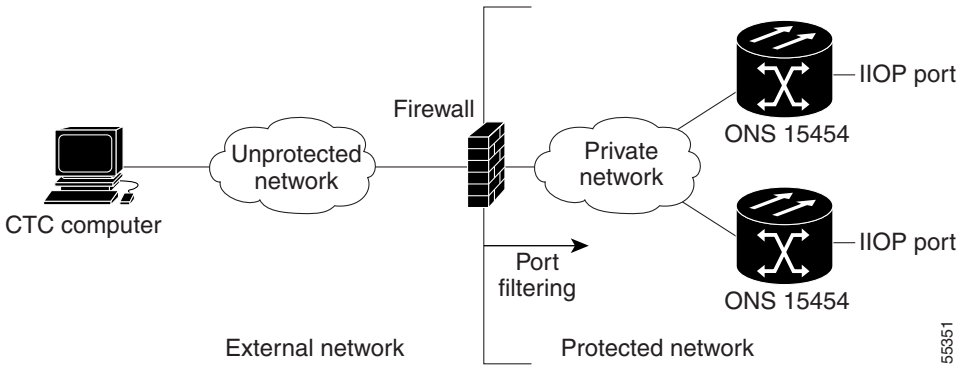
Purpose	This procedure provisions ONS 15454s and CTC computers for access through firewalls.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node that is behind the firewall. See the "DLP-A60 Log into CTC" task on page 3-24 for instructions. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A67 Provision the IIOP Listener Port on the ONS 15454" task on page 4-20.

Figure 4-5 shows ONS 15454s in a protected network and the CTC computer in an external network. For the computer to access the ONS 15454s, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15454.

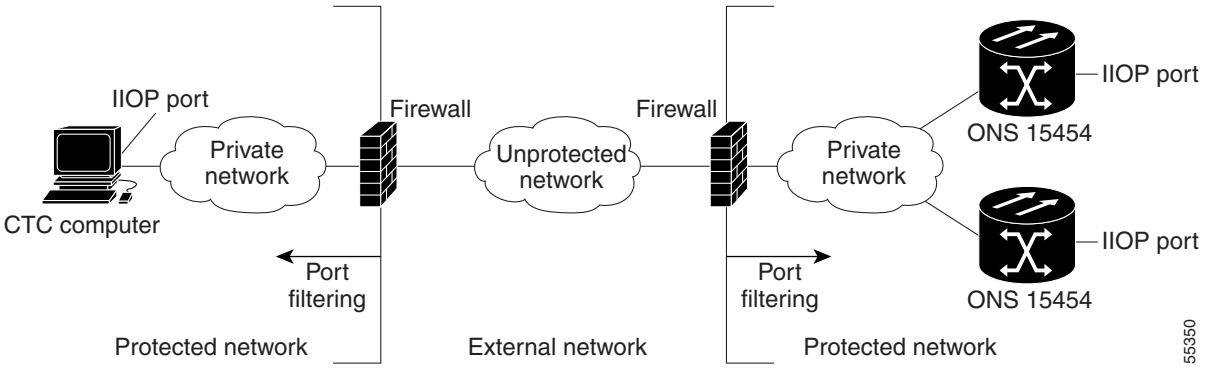
Figure 4-5 Nodes Behind a Firewall



Step 3 If the CTC computer resides behind a firewall, complete the "DLP-A68 Provision the IIOP Listener Port on the CTC Computer" task on page 4-22.

Figure 4-6 shows a CTC computer and ONS 15454 behind firewalls. For the computer to access the ONS 15454, you must provision the IIOP port on the CTC computer and on the ONS 15454.

Figure 4-6 CTC Computer and ONS 15454s Residing Behind Firewalls



Stop. **You have completed this procedure**.

DLP-A67 Provision the IIOP Listener Port on the ONS 15454

Purpose	This task sets the IIOP listener port on the ONS 15454, which enables you to access ONS 15454s that reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the Enable Proxy Server on port 1080 check box is checked, CTC will use port 1080 and ignore the configured IIOP port setting. If Enable Proxy Server is subsequently unchecked, the configured IIOP listener port will be used.

Step 1 In node view, click the **Provisioning > Network > General** tabs.

Step 2 In the TCC CORBA (IIOP) Listener Port area, choose a listener port option:

- Default - TCC Fixed—Uses Port 57790 to connect to ONS 15454s on the same side of the firewall or if no firewall is used (default). This option can be used for access through a firewall if Port 57790 is open.
- Standard Constant—Uses Port 683, the CORBA default port number.
- Other Constant—If Port 683 is not used, type the IIOP port specified by your firewall administrator. The port cannot use any of the ports shown in Table 4-2.

Table 4-2 Ports Used by the TCC2 Cards

Port	Function
0	Reserved
21	FTP control
23	Telnet
80	HTTP
111	rpc (not used; but port is in use)
513	rlogin (not used; but port is in use)
=<1023	Default CTC listener ports
1080	Proxy server
2001-2017	I/O card telnet
2018	DCC processor on active TCC2
2361	TL1
3082	TL1
3083	TL1
5001	Bidirectional line switched ring (BLSR) server port
5002	BLSR client port
7200, 7209, 7210	SNMP input port
9100	EQM port
9101	EQM port 2
9401	TCC2 boot port
9999	Flash manager
57790	Default TCC2 listener port

Step 3 Click **Apply**.

Step 4 When the Change Network Configuration message appears, click **Yes**.

Both ONS 15454 TCC2s reboot, one at a time. The reboot takes approximately 15 minutes. See Table 4-1 on page 4-12.

Step 5 Return to your originating procedure (NTP).

DLP-A68 Provision the IIOP Listener Port on the CTC Computer

Purpose	This task selects the IIOP listener port on CTC.
Tools/Equipment	IIOP listener port number from LAN or firewall administrator.
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required only if the computer running CTC resides behind a firewall.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Firewall** tab.

Step 3 In the CTC CORBA (IIOP) Listener Port area, choose a listener port option:

- Default - Variable—Use to connect to ONS 15454s from within a firewall or if no firewall is used (default).
- Standard Constant—Use Port 683, the CORBA default port number.
- Other Constant—If Port 683 is not used, enter the IIOP port defined by your administrator.

Step 4 Click **Apply**. A warning appears telling you that the port change will apply during the next CTC login.

Step 5 Click **OK**.

Step 6 In the Preferences dialog box, click **OK**.

Step 7 To access the ONS 15454 using the IIOP port, log out of CTC then log back in. (To log out, choose **Exit from the File menu.**)

Step 8 Return to your originating procedure (NTP).

NTP-A28 Set Up Timing

Purpose	This procedure provisions the ONS 15454 timing.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the ONS 15454 is a DWDM or hybrid (TDM and DWDM) node, do not complete this procedure if you are provisioning the node for line timing with an OSCM or OSC-CSM card as a timing reference. The OSCM and OSC-CSM are not available for selection on the Timing subtab until you complete the "NTP-A268 Install the DWDM or Hybrid Node Cards" procedure on page 5-3. If the DWDM or hybrid node timing is external, that is, timing is derived from a BITS source wired to the backplane, you can complete this procedure now.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will set up timing. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A69 Set Up External or Line Timing" task on page 4-23 if an external building integrated timing supply (BITS) source is available. This is the common SONET timing setup procedure.

Step 3 If you cannot complete Step 2 (an external BITS source is not available), complete the "DLP-A70 Set Up Internal Timing" task on page 4-25. This task can only provide Stratum 3 timing.

Note For information about SONET timing, refer to the *Cisco ONS 15454 Reference Manual* or to Telcordia GR-253-CORE.

Stop. **You have completed this procedure**.

DLP-A69 Set Up External or Line Timing

Purpose	This task defines the SONET timing source (external or line) for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 In the General Timing area, complete the following information:

- Timing Mode—Choose **External** if the ONS 15454 derives its timing from a BITS source wired to the backplane pins; choose **Line** if timing is derived from an OC-N card (non-DWDM nodes) or OSC card (DWDM nodes) that is optically connected to the timing node. A third option, Mixed, allows you to set external and line timing references.

  Note Because Mixed timing might cause timing loops, Cisco does not recommend its use. Use this mode with care.

- SSM Message Set—Choose a synchronization status messaging (SSM) message set. All ONS 15454s can translate Generation 2 message sets, so choose Generation 2 if the ONS 15454 is connected to other ONS 15454s. Choose Generation 1 only when the ONS 15454 is connected to equipment that does not support Generation 2. If a node that has its SSM Message Set set to Generation 1 receives a Generation 2 message, it maps the message down to the next available Generation 1 message. The transit node clock (TNC) and ST3E (Stratum 3E) will become an ST3 (Stratum 3).

- Quality of RES—If your timing source supports the reserved S1 byte, set the timing quality here. (Most timing sources do not use RES.) Qualities are displayed in descending quality order as ranges. For example, ST3<RES<ST2 means the timing reference is higher than a Stratum 3 and lower than a Stratum 2. Refer to the *Cisco ONS 15454 Reference Manual* for more information about SSM, including definitions of the SONET timing levels.
- Revertive—Select this check box if you want the ONS 15454 to revert to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- Revertive Time—If Revertive is checked, choose the amount of time the ONS 15454 will wait before reverting to its primary timing source. Five minutes is the default.

Step 3 In the BITS Facilities area, complete the following information:

Note The BITS Facilities section sets the parameters for your BITS-1 and BITS-2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

- BITS In State—If Timing Mode is set to External or Mixed, set the BITS In State for BITS-1 and/or BITS-2 to **IS** (in service) depending whether one or both BITS input pin pairs on the backplane are connected to the external timing source. If Timing Mode is set to Line, set the BITS In State to **OOS** (out of service).
- BITS Out State—If equipment is connected to the node's BITS output pins on the backplane and you want to time the equipment from a node reference, set the BITS Out State for BITS-1 and/or BITS-2 to **IS**, depending on which BITS Out pins are used for the external equipment. If equipment is not attached to the BITS output pins, set the BITS Out State to **OOS**.

Step 4 If the BITS In State for BITS-1 and BITS-2 is set to OOS, continue with Step 5. If the BITS In State is set to IS for either BITS-1 or BITS-2, complete the following information:

- Coding—Set to the coding used by your BITS reference, either B8ZS (binary 8-zero substitution) or AMI (alternate mark inversion).
- Framing—Set to the framing used by your BITS reference, either ESF (Extended Super Frame) or SF (D4) (Super Frame).
- Sync Messaging—Check to enable SSM. SSM is not available if Framing is set to SF (D4).
- AIS Threshold—If SSM is disabled or SF (D4) is used, set the quality level where a node sends an alarm indication signal (AIS) from the BITS-1 Out and BITS-2 Out backplane pins. An AIS is raised when the optical source for the BITS reference falls to or below the SSM quality level defined in this field.
- LBO—If you are timing an external device connected to the BITS Out pins, set the distance between the device and the ONS 15454. Options are: 0-133 ft. (default), 124-266 ft., 267-399 ft., 400-533 ft., and 534-655 ft. Line build out (LBO) relates to the BITS cable length.

Step 5 In the Reference Lists area, complete the following information:

Note Reference Lists defines up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out pins on the backplane. If you attach equipment to BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

Note If a 1+1 node will use line timing, make a working OC-N card the Ref-X timing source. The system will automatically choose the corresponding protect OC-N card as the Ref-X protect timing source. This will be visible in the Maintenance > Timing tab.

- NE Reference—Allows you to define three timing references (Ref 1, Ref 2, Ref 3). The node uses Reference 1 unless a failure occurs to that reference, in which case the node uses Reference 2. If Reference 2 fails, the node uses Reference 3, which is typically set to Internal Clock. Reference 3 is the Stratum 3 clock provided on the TCC2 card. The options displayed depend on the Timing Mode setting.
  - If the Timing Mode is set to External, your options are BITS-1, BITS-2, and Internal Clock.
  - If the Timing Mode is set to Line, your options are the node's working OC-N cards (non-DWDM nodes) or OSC cards (DWDM nodes) and Internal Clock. Choose the cards/ports that are directly or indirectly connected to the node wired to the BITS source, that is, the node's trunk (span) cards. Set Reference 1 to the trunk card that is closest to the BITS source. For example, if Slot 5 is connected to the node wired to the BITS source, choose Slot 5 as Reference 1.
  - If the Timing Mode is set to Mixed, both BITS and OC-N cards are available, allowing you to set a mixture of external BITS and OC-N trunk cards as timing references.
- BITS-1 Out/BITS-2 Out—Sets the timing references for equipment wired to the BITS Out backplane pins. BITS-1 Out and BITS-2 Out are enabled when BITS-1 and BITS-2 facilities are put in service. If Timing Mode is set to external, choose the OC-N card used to set the timing. If Timing Mode is set to Line, you can choose an OC-N card or choose NE Reference to have the BITS-1 Out and/or BITS-2 Out follow the same timing references as the NE.

Step 6 Click **Apply**.

Note Refer to the *Cisco ONS 15454 Troubleshooting Guide* for timing-related alarms.

Step 7 Return to your originating procedure (NTP).

DLP-A70 Set Up Internal Timing

Purpose	This task sets up internal timing (Stratum 3) for an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed (use only if a BITS source is not available)
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Internal timing is Stratum 3 and not intended for permanent use. All ONS 15454s should be timed to a Stratum 2 or better primary reference source.

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 In the General Timing area, enter the following:

- Timing Mode—Set to External.
- SSM Message Set—Set to Generation 1.
- Quality of RES—Does not apply to internal timing.
- Revertive—Does not apply to internal timing.
- Revertive Time—Does not apply to internal timing.

Step 3 In the BITS Facilities area, change BITS In State and BITS Out State to **OOS**. Disregard the other BITS Facilities settings; they are not relevant to internal timing.

Step 4 In the Reference Lists area, enter the following information:

- NE Reference
  - Ref 1—Set to Internal Clock.
  - Ref 2—Set to Internal Clock.
  - Ref 3—Set to Internal Clock.
- BITS-1 Out/BITS-2 Out—Set to None.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

NTP-A170 Create Protection Groups

Purpose	This procedure creates ONS 15454 card protection groups.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

Step 2 Complete one or more of the following tasks depending on the protection groups you want to create:

- DLP-A71 Create a 1:1 Protection Group, page 4-28
- DLP-A72 Create a 1:N Protection Group, page 4-29
- DLP-A73 Create a 1+1 Protection Group, page 4-30
- DLP-A252 Create a Y-Cable Protection Group, page 4-32

Table 4-3 describes the protection types available on the ONS 15454.

Table 4-3 Protection Types

Type	Cards	Description and Installation Requirements
1:1	DS1-14 DS3-12 DS3-12E EC1-12 DS3XM-6	Pairs one working card with one protect card. The protect card should be installed in an odd-numbered slot and the working card in an even-numbered slot next to the protect slot towards the TCC2, for example: protect in Slot 1, working in Slot 2; protect in Slot 3, working in Slot 4; protect in Slot 15, working in Slot 14. 1:1 protection can be revertive or nonrevertive. For more information, refer to the "Card Protection" chapter in the *ONS 15454 Reference Manual*.
1:N	DS1N-14 DS3N-12 DS3N-12E	Assigns one protect card for several working cards. The maximum is 1:5. Protect cards (DS1N-14, DS3N-12, DS3N-12E) must be installed in Slots 3 or 15 and the cards they protect must be on the same side of the shelf. Protect cards must match the cards they protect. For example, a DS1N-14 can only protect DS1-14 or DS1N-14 cards. If a failure clears, traffic reverts to the working card after the reversion time has elapsed. For more information, refer to the "Card Protection" chapter in the *ONS 15454 Reference Manual*.
1+1	Any OC-N	Pairs a working OC-N card/port with a protect OC-N card/port. For multiport OC-N cards, the protect port must match the working port on the working card. For example, Port 1 of an OC-3 card can only be protected by Port 1 of another OC-3 card. The ports on multiport cards must be either working or protect. You cannot mix working and protect ports on the same card. Cards do not need to be in adjoining slots. 1+1 protection can be revertive or nonrevertive, bidirectional or unidirectional.
Y Cable	MXP_2.5_10G TXP_MR_10G TXP_MR_2.5G	Pairs a working transponder or muxponder card/port with a protect transponder or muxponder card/port. The protect port must be on a different card than the working port and it must be the same card type as the working port. The working and protect port numbers must be the same, that is, Port 1 can only protect Port 1, Port 2 can only protect Port 2, etc.
Splitter	TXPP_MR_2.5G	Splitter protection is automatically provided with the TXPP_MR_2.5G card.
Unprotected	Any	Unprotected cards can cause signal loss if a card fails or incurs a signal error. However, because no card slots are reserved for protection, unprotected schemes maximize the service available for use on the ONS 15454. Unprotected is the default protection type.

Stop. You have completed this procedure.

DLP-A71 Create a 1:1 Protection Group

Purpose	This task creates a 1:1 electrical card protection group.
Tools/Equipment	Redundant DS-1, DS-3, EC-1, or DS3XM-6 cards should be installed in the shelf, or the ONS 15454 slots must be provisioned for two of these cards.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards required for 1:1 protection are installed according to requirements specified in Table 4-3.

Step 2 In node view, click the **Provisioning** > **Protection** tabs.

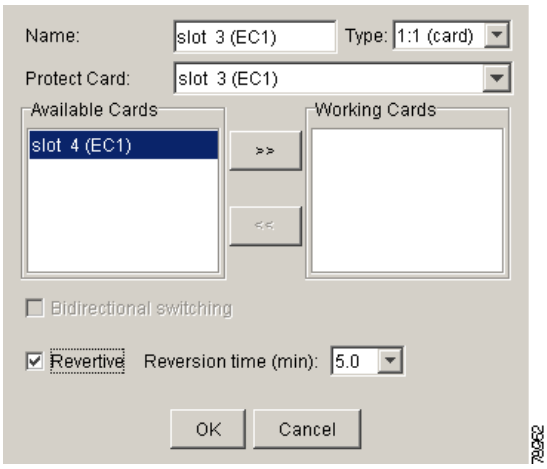
Step 3 Click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (“) characters.
- Type—Choose **1:1** from the drop-down menu.
- Protect Card—Choose the protect card from the drop-down menu. The menu displays cards available for 1:1 protection. If no cards are available, no cards appear in the list.

After you choose the protect card, the card available for protection appear in the Available Cards list, as shown in Figure 4-7. If no cards are available, no cards appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Slot” task on page 5-5.

Figure 4-7 Creating a 1:1 Protection Group



Step 5 From the Available Cards list, choose the card that will be protected by the card selected in the Protect Card drop-down menu. Click the top arrow button to move each card to the Working Cards list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Not available for 1:1 protection.
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions remain corrected for the amount of time entered in the Reversion Time field.
- Reversion time—If Revertive is checked, choose the reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card after conditions causing the switch are cleared.

Step 7 Click **OK**, then click **Yes** in the confirmation dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-A72 Create a 1:N Protection Group

Purpose	This task creates a DS-1 or DS-3 1:N protection group.
Tools/Equipment	DS1N-14, DS3N-12, or DS3N-12E (protect cards) in Slot 3 or Slot 15; DS1-14, DS3-12, or DS3-12E (working cards) installed on either side of a corresponding protect card.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards are installed according to the 1:N requirements specified in Table 4-3 on page 4-27.

Step 2 Click the **Provisioning** > **Protection** tabs.

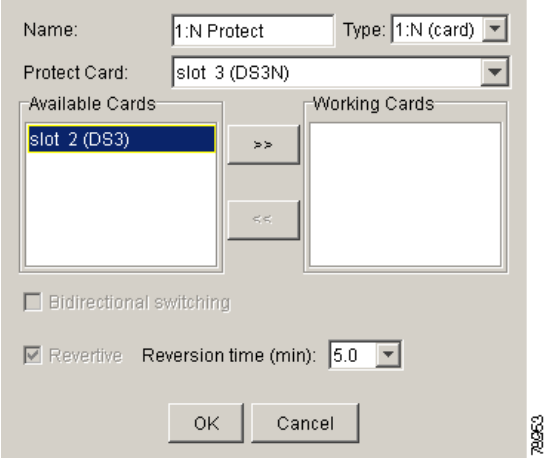
Step 3 In the Protection Groups area, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (“) characters.
- Type—Choose **1:N** from the drop-down menu.
- Protect Card—Choose the protect card from the drop-down menu. The menu displays DS1N-14, DS3N-12, or DS3N-12E cards installed in Slots 3 or 15. If these cards are not installed, no cards appear in the drop-down menu.

After you choose the protect card, a list of cards available for protection appear in the Available Cards list, as shown in Figure 4-8. If no cards are available, no cards appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Slot” task on page 5-5.

Figure 4-8 Creating a 1:N Protection Group



Step 5 From the Available Cards list, choose the cards that will be protected by the card selected in the Protect Card drop-down menu. Click the top arrow button to move each card to the Working Cards list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Not available for 1:N protection.
- Revertive—Always enabled for 1:N protection groups.
- Reversion time—Click **Reversion time** and select a reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card after conditions causing the switch are cleared.

Step 7 Click **OK**, then click **Yes** in the confirmation dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-A73 Create a 1+1 Protection Group

Purpose	This task creates a 1+1 protection group for any OC-N card/port (OC-3, OC-3-8, OC-12, OC-12-4, OC-48, OC-48 AS, and OC-192).
Tools/Equipment	Installed OC-N cards or preprovisioned slots
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards are installed according to 1+1 requirements specified in Table 4-3 on page 4-27.

Step 2 In node view, click the **Provisioning** > **Protection** tabs.

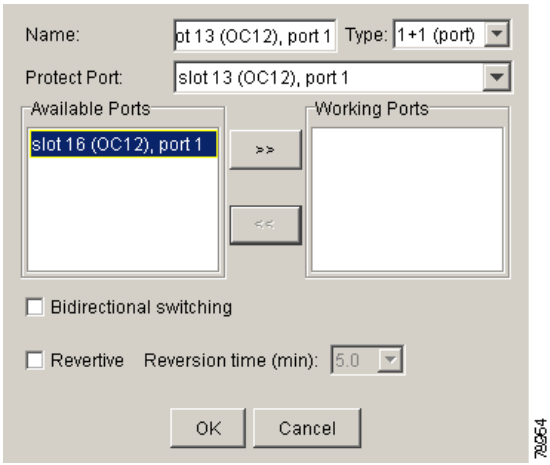
Step 3 In the Protection Groups area, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (“) characters.
- Type—Choose **1+1** from the drop-down menu.
- Protect Port—Choose the protect port from the drop-down menu. The menu displays the available OC-N ports, as shown in Figure 4-9. If OC-N cards are not installed, no ports appear in the drop-down menu.

After you choose the protect port, a list of ports available for protection appear in the Available Ports list, as shown in Figure 4-9. If no cards are available, no ports appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Slot” task on page 5-5.

Figure 4-9 Creating a 1+1 Protection Group



Step 5 From the Available Ports list, choose the port that will be protected by the port you selected in the Protect Port field. Click the top arrow button to move each port to the Working Ports list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Check this check box if you want both Tx and Rx signals to switch to the protect port when a failure occurs to one signal. Leave unchecked if you want only the failed signal to switch to the protect port.
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions remain corrected for the amount of time entered in the Reversion Time field.
- Reversion time—If Revertive is checked, choose a reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the traffic reverts to the working card after conditions causing the switch are cleared.

Step 7 Click **OK**.

Step 8 Return to your originating procedure (NTP).

DLP-A252 Create a Y-Cable Protection Group

Purpose	This task creates a Y-cable protection group between the client ports of two transponder (TXP_MR_10G or TXP_MR_2.5G) or two muxponder (MXP_2.5G_10G) cards.
Tools/Equipment	Installed transponder or muxponder cards or preprovisioned slots.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Loss of Pointer Path (LOP-P) alarms can occur on a split signal if the ports are not in a Y-cable protection group.

Step 1 Verify that the transponder or muxponder cards are installed according to the Y-cable requirements specified in Table 4-3 on page 4-27.

Step 2 In node view, click the **Provisioning > Protection** tabs.

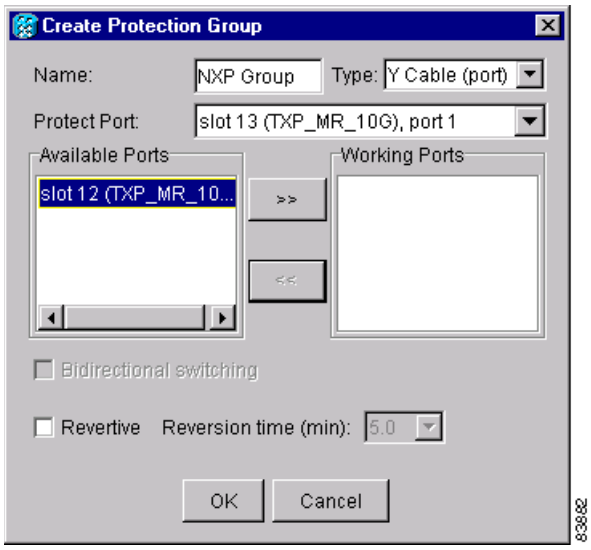
Step 3 In the Protection Groups area, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question mark (?), backslash (\), or double quote (“) characters.
- Type—Choose **Y Cable** from the drop-down menu.
- Protect Port—Choose the protect port from the drop-down menu. The menu displays the available transponder or muxponder ports, as shown in Figure 4-9. If transponder or muxponder cards are not installed, no ports appear in the drop-down menu.

After you choose the protect port, a list of ports available for protection appear in the Available Ports list, as shown in Figure 4-10. If no cards are available, no ports appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Slot” task on page 5-5.

Figure 4-10 Creating a Y-Cable Protection Group



Step 5 From the Available Ports list, choose the port that will be protected by the port you selected in Protect Ports. Click the top arrow button to move each port to the Working Ports list.

Step 6 Complete the remaining fields:

- Revertive—Check this check box if you want traffic to revert to the working port after failure conditions remain corrected for the amount of time entered in the Reversion Time field.
- Reversion time—If Revertive is checked, select a reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

Step 7 Click **OK**.

Step 8 Return to your originating procedure (NTP).

NTP-A256 Set Up SNMP

Purpose	This procedure provisions the SNMP parameters so that you can use SNMP management software with the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	Required if SNMP is used at your installation.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to set up SNMP. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > SNMP** tabs.

Step 3 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If this box is not checked, SET requests are rejected.

Step 4 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the **Enable SNMP Proxy** check box located on the SNMP tab.

Step 5 Click **Apply**.

Step 6 After clicking either one or both option check boxes, click **Create** in the Trap Destinations area.

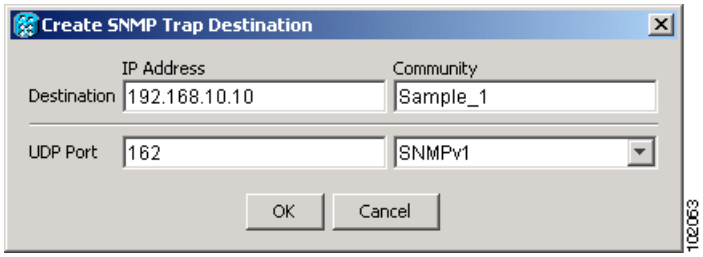
Step 7 If you are only allowing SNMP sets, complete the following in the Create SNMP Trap Destination dialog box (Figure 4-11):

- Destination IP Address—Type the IP address of your network management system. If the node you are logged into is an ENE, set the destination address to the GNE.
- Community—Type the SNMP community name. For a description of SNMP community names, refer to the SNMP information in the *Cisco ONS 15454 Reference Manual*.

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the network management system (NMS).

- UDP Port—The default User Datagram Protocol (UDP) port for SNMP is 162. If the node is an ENE in a proxy server network, the UDP port must be set to the GNE's SNMP relay port, which is 391 for SNMPv1.
- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

Figure 4-11 Creating an SNMP Trap Without Proxy



Step 8 Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.

Step 9 Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.

Step 10 If you are enabling SNMP proxy, the dialog box contains additional fields that allow you to set three relays addresses for sending SNMP trap error counts back to NE. To complete these relay IP address fields:

a. Click the first trap destination IP address. The address and its community name appear in the Destination fields.

b. Enter up to three SNMP Proxy relay addresses and community names in the fields for Relay A, Relay B, and Relay C.

Note The community names specified for each relay node must match one of the provisioned SNMP community names in the NE.

Note The SNMP proxy directs SNMP traps from this node through IpA to IpB to IpC to the trap destination. Ensure that you enter the IP addresses in the correct order so that this sequence runs correctly.

Step 11 Click **OK**.

Stop. **You have completed this procedure**.