CHAPTER 4

Turn Up a Node

This chapter explains how to provision a single Cisco ONS 15600 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.

Before You Begin

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

- Chapter 1, “Install the Bay and Backplane Connections”
- 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 a list of its tasks (DLPs).

1. NTP-E21 Verify Card Installation, page 4-2—Complete this procedure first.
2. NTP-E26 Create Users and Assign Security, page 4-3—Continue with this procedure to create Cisco Transport Controller (CTC) users and assign their security levels.
3. NTP-E22 Set Up Date, Time, and Contact Information, page 4-4—Continue with this procedure to set the node name, date, time, location, and contact information.
4. NTP-E189 Set Power Monitor Thresholds, page 4-6—Continue with this procedure on a node with a CAP2 installed to provision power thresholds within a –48 volts direct current (VDC) environment.
5. NTP-E23 Set Up CTC Network Access, page 4-7——Continue with this procedure to provision the IP address, default router, subnet mask, and network configuration settings.
6. NTP-E198 Set Up the ONS 15600 in EMS Secure Access, page 4-7—Continue with this procedure to connect the CTC in secure mode.
7. NTP-E94 Set Up the ONS 15600 for Firewall Access, page 4-8—Continue with this procedure if the ONS 15600 will be accessed behind firewalls.
8. NTP-E25 Create FTP Host, page 4-9 -- Continue with this procedure if to create FTP host for ENE database backup.
9. NTP-E24 Set Up Timing, page 4-10—Continue with this procedure to set up SONET timing references.
10. NTP-E26 Create a 1+1 Protection Group, page 4-11—Complete as needed to set up 1+1 protection groups for ONS 15600 optical cards.

11. NTP-E27 Set Up SNMP, page 4-13—Complete as needed to set up Simple Network Management Protocol (SNMP).
12. NTP-E28 Set the User Code for Card Inventory, page 4-14—Complete as needed to create a user code that helps identify the SSXC, TSC, and optical (traffic) cards.
13. NTP-E29 Configure a Node Using an Existing Database, page 4-14—Complete as needed to download the provisioning database file from one node onto a designated node.
14. NTP-E48 Set External Alarms and Controls, page 4-16—Complete as needed to provision external alarm reporting, assign external alarms to virtual wires, and view external alarms for ONS 15600 nodes, ONS 15310-CL nodes, ONS 15310-MA nodes, and ONS 15600 nodes.
15. NTP-E174 Provision OSI, page 4-16—Complete this procedure if the ONS 15600 will be connected in networks with network elements (NEs) that are based on the Open System Interconnection (OSI) protocol stack. This procedure provisions the TID Address Resolution Protocol (TARP), OSI routers, manual area addresses, subnetwork points of attachment, and IP over OSI tunnels.
16. NTP-E200 Provision Node for SNMPv3, page 4-17—Complete as needed to set up Simple Network Management Protocol version 3 (SNMPv3)

NTP-E21 Verify Card Installation

Purpose	This procedure verifies that the ONS 15600 node is ready for turn-up.
Tools/Equipment	None
Prerequisite Procedures	Chapter 1, “Install the Bay and Backplane Connections” Chapter 2, “Install Cards and Fiber-Optic Cable”
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Verify that the TSC cards are installed in Slots 5 and 10.

Step 2 Verify that the ACT/STBY LED on the active TSC is green. The ACT/STBY LED will not be on for the standby TSC.

Note If the TSCs are not installed or their LEDs are not on as described, do not continue. See Chapter 2, “Install Cards and Fiber-Optic Cable,” or refer to the *Cisco ONS 15600 Troubleshooting Guide* to resolve installation problems before proceeding.

Step 3 Verify that the cross-connect (SSXC) cards are installed in Slots 6 and 8. The SSXC card faceplate extends to cover Slots 7 and 9, respectively.

Step 4 Verify that the SRV LED is illuminated on both SSXC cards.

Note If the SSXC cards are not installed, or their LEDs are not on as described, do not continue with the procedure. See Chapter 2, “Install Cards and Fiber-Optic Cable,” or refer to the *Cisco ONS 15600 Troubleshooting Guide* to resolve installation problems before proceeding.

Step 5 Verify that the OC-N cards are installed in the slots designated by your site plan. Slots 1 to 4 and 11 to 14 are used for all optical cards.

Step 6 Verify that fiber-optic cables are installed and connected to the locations indicated in the site plan.

Step 7 Verify that fiber is routed correctly in the shelf assembly.

Step 8 Verify that the SSXC cards are working:

a. Complete the "DLP-E26 Log into CTC" task on page 16-31 at the node that you will turn up.

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

c. Click **Run Diagnostics Test**.

- If errors exist, the Cross Connect Diagnostics Error box opens to list the errors. Click **Close**.
- If no errors exist, click **OK** to close the confirmation dialog box.

Note You must run the diagnostics test before the optical cards are provisioned.

Step 9 Set the optical power received threshold for each optical card. See the "DLP-E124 Set the Optical Power Received Nominal Value" task on page 17-22 for instructions.

Step 10 If all cards and fiber are installed in the ONS 15600 shelf as described in Steps 1 through 9, continue with the "NTP-E26 Create Users and Assign Security" procedure on page 4-3.

Note If cards are not installed or the LEDs are not shown as described, do not continue. Go to Chapter 2, "Install Cards and Fiber-Optic Cable" or the *CCisco ONS 15600 Troubleshooting Guide* to resolve the installation problems before continuing with shelf turn up.

Stop. You have completed this procedure.

NTP-E26 Create Users and Assign Security

Purpose	This procedure creates ONS 15600 users and assigns security levels.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 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-E26 Log into CTC" task on page 16-31 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 15600 can be used to set up other ONS 15600 users. You can add up to 500 users to one ONS 15600.

Step 2 Complete the "DLP-E35 Create a New User on a Single Node" task on page 16-46 or the "DLP-E36 Create a New User on Multiple Nodes" task on page 16-47, as needed.

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

Step 3 As needed, complete the "DLP-E268 Configure the Node for RADIUS Authentication" task on page 18-81. Remote Authentication Dial In User Service (RADIUS) validates remote users trying to connect to the network.

Stop. You have completed this procedure.

NTP-E22 Set Up 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-E21 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-E26 Log into CTC" task on page 16-31 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/TID—Enter 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—(Optional) Enter the name of the node contact person and the phone number, up to 255 characters.
- Latitude—(Optional) Enter the node latitude: N (North) or S (South), degrees, and minutes.
- Longitude—(Optional) Enter the node longitude: E (East) or W (West), degrees, and minutes.

Tip You can also position nodes manually in network view. Press Ctrl while you drag and drop the node icon. To create the same network map visible for all ONS 15600 users, complete the "NTP-E86 Create a Logical Network Map" procedure on page 5-36.

Note The latitude and longitude values only indicate the geographical position of the nodes in the actual network and not the CTC node position.

- Description—Enter 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 15600 will use these fields for alarm dates and times. By default, CTC displays all alarms in the CTC computer time zone for consistency. To change the display to the node time zone, complete the "DLP-E46 Display Events Using Each Node's Time Zone" task on page 16-56.

  Note Using an NTP or SNTP server ensures that all ONS 15600 network nodes use the same date and time reference. The server synchronizes node time after power outages or software upgrades.

  If you check the Use NTP/SNTP Server check box, complete the following fields:

  - Use NTP/SNTP Server—Type the IP address of the primary NTP/SNTP server connected to the ONS 15600 or of another ONS 15600/15454/15310-CL/15310-MA as GNE with NTP/SNTP enabled that is connected to the ONS 15600 ENE.
  - Backup NTP/SNTP Server—Type the IP address of the secondary NTP/SNTP server connected to the ONS 15600 or of another ONS 15600/15454/15310-CL/15310-MA as GNE with NTP/SNTP enabled that is connected to the ONS 15600 ENE.

    When the primary NTP/SNTP server fails or is not reachable, the node uses the secondary NTP/SNTP server to synchronize its date and time. If both the primary and secondary NTP/SNTP servers fail or are not reachable, an SNTP-FAIL alarm is raised. The node checks for the availability of the primary or secondary NTP/SNTP server at regular intervals until it can get the time from any one of the NTP/SNTP servers. After the node gets the time from any one server, it synchronizes its date and time with the server's date and time and the SNTP-FAIL alarm is cleared. For each retry and resynchronization, the node checks the availability of the primary NTP/SNTP server first, followed by the secondary NTP/SNTP server. The node synchronizes its date and time every hour.

    Note You will not be able to identify which NTP/SNTP server is being used for synchronization.

  If you check Gateway Network Element (GNE) for the ONS 15600 SOCKS proxy server (see the "DLP-E30 Provision IP Settings" task on page 16-37), external ONS 15600s must reference the gateway ONS 15600 for NTP/SNTP timing. For more information about the ONS 15600 gateway settings, refer to the *Cisco ONS 15600 Reference Manual*.

  Note In ONS 15600 Software Release 9.0 and later, you can configure an IPv6 address for an NTP/SNTP server, in addition to an IPv4 address.

Caution If you reference another ONS 15600 for the NTP/SNTP server, make sure the second ONS 15600 references an NTP/SNTP server and not the first ONS 15600 (that is, do not create an NTP/SNTP timing loop by having two ONS 15600s reference each other).

- Date—If Use NTP/SNTP Server is not selected, enter 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 selected, enter the current time in the format hh:mm:ss, for example, 11:24:58. The ONS 15600 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 popup 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).

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-E189 Set Power Monitor Thresholds" procedure on page 4-6.

Stop. You have completed this procedure.

NTP-E189 Set Power Monitor Thresholds

Purpose	This procedure provisions extreme high, extreme low, and low input battery power thresholds within a –48 volts direct current (VDC) environment. When the thresholds are crossed, the TSC generates warning alarms in CTC. You must have a customer access panel version 2 (CAP2) installed to be able to set power thresholds.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 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-E26 Log into CTC" task on page 16-31 at the node where you want to set power monitor thresholds. 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 ELWBATVG(Vdc) drop-down list.

Step 4 To change the low battery voltage threshold in 0.5 VDC increments, choose a voltage from the LWBATVG(Vdc) drop-down list.

Step 5 To change the high battery voltage threshold in 0.5 VDC increments, choose a voltage from the HIBATVG(Vdc) drop-down list.

Step 6 To change the extreme high battery voltage threshold in 0.5 VDC increments, choose a voltage from the EHIBATVG(Vdc) drop-down list.

Step 7 Click **Apply**.

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

NTP-E23 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, (Internet Inter-Orb Protocol) IIOP listener port, SOCKS proxy server settings, static routes, and Open Shortest Path First (OSPF) protocol, and designated SOCKS servers
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 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-E26 Log into CTC" task on page 16-31. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-E30 Provision IP Settings" task on page 16-37 to provision the ONS 15600 IP address, subnet mask, default router, DHCP server, IIOP listener port, and SOCKS proxy server settings.

Step 3 If static routes are needed, complete the "DLP-E31 Create a Static Route" task on page 16-40. Refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15600 Reference Manual* for more information about static routes.

Step 4 If the ONS 15600 is connected to a LAN or WAN that uses OSPF and you want to share routing information between the LAN/WAN and the ONS network, complete the "DLP-E32 Set Up or Change Open Shortest Path First Protocol" task on page 16-41.

Step 5 Complete the "DLP-E294 Provision the Designated SOCKS Servers" task on page 18-118 after the network is provisioned and one or more of the following conditions exist:

- SOCKS proxy is enabled.
- The ratio of ENEs to GNEs is greater than eight to one.
- Most ENEs do not have LAN connectivity.

Stop. You have completed this procedure.

NTP-E198 Set Up the ONS 15600 in EMS Secure Access

Purpose	This procedure provisions ONS 15600s and CTC computers for secure access.
Tools/Equipment	None
Prerequisite Procedures	NTP-E23 Set Up CTC Network Access, page 4-7
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > Security > Access** pane.

Step 2 Under the **EMS Access** area, change the **Access State** to **Secure**.

Step 3 Click **Apply**. The CTC disconnects and reconnects through a secure socket connection.

Step 4 To create a secure connection, enter **https://node-address**.

Note After setting up a CTC connection in secure mode, http requests are automatically redirected to https mode.

Step 5 A first time connection is authenticated by the **Website Certification is Not Known** dialog box. Accept the certificate and click **OK**. The **Security Error: Domain Name Mismatch** dialog box appears. Click **OK** to continue.

Stop. You have completed this procedure.

NTP-E94 Set Up the ONS 15600 for Firewall Access

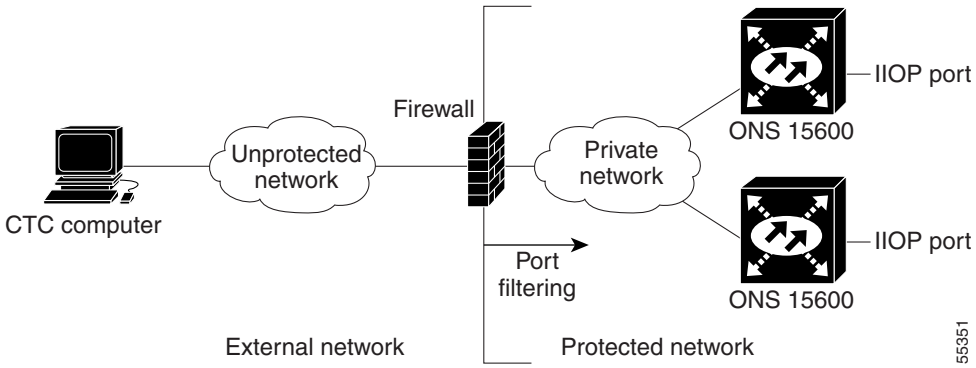
Purpose	This procedure provisions ONS 15600s and CTC computers for access through firewalls.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31. If you are already logged in, continue with Step 2.

Step 2 If the ONS 15600 resides behind a firewall, complete the "DLP-E125 Provision the IIOP Listener Port on the ONS 15600" task on page 17-22.

Figure 4-1 shows an ONS 15600 in a protected network and the CTC computer in an external network. For the computer to access the ONS 15600s, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15600.

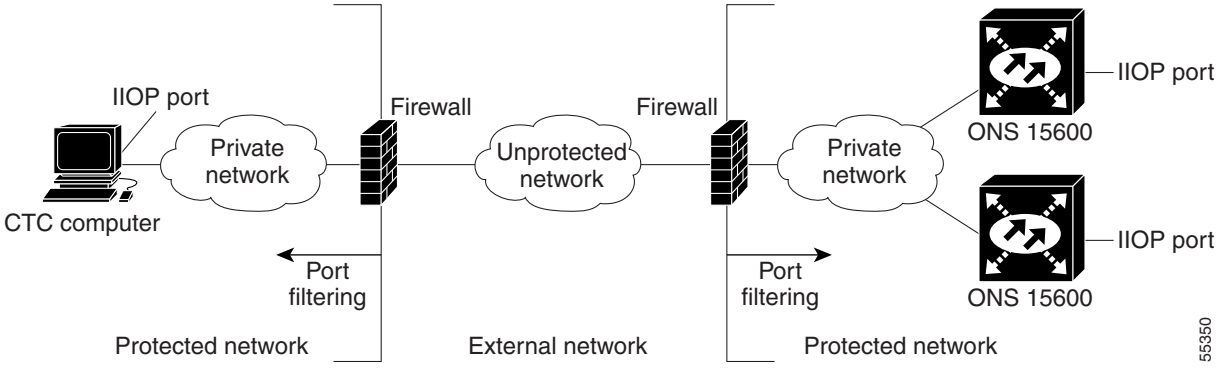
Figure 4-1 Nodes Behind a Firewall



Step 3 If the CTC computer resides behind a firewall, complete the "DLP-E126 Provision the IIOP Listener Port on the CTC Computer" task on page 17-23.

Figure 4-2 shows a CTC computer and ONS 15600 behind firewalls. For the computer to access the ONS 15600, you must provision the IIOP port on the CTC computer and on the ONS 15600.

Figure 4-2 CTC Computer and ONS 15600s Residing Behind Firewalls



Stop. You have completed this procedure.

NTP-E25 Create FTP Host

Purpose	This procedure provisions an FTP Host that you can use to perform database backup and restore or software download to an End Network Element (ENE) when proxy or firewall is enabled.
Tools/Equipment	None
Prerequisite Procedures	NTP-E23 Set Up CTC Network Access, page 4-7 NTP-E94 Set Up the ONS 15600 for Firewall Access, page 4-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31. If you are already logged in, continue with Step 2.

Step 2 If you want to turn on the ONS 15600 secure mode, which allows two IPv4 addresses to be provisioned for the node if TCC2P cards are installed, complete the NTP-E198 Set Up the ONS 15600 in EMS Secure Access, page 4-7. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15600 SDH Reference Manual* for information about secure mode.

Step 3 In Node view, click the **Provisioning > Network > FTP Hosts** tabs.

Step 4 Click **Create**.

Step 5 Enter a valid IP address in the FTP Host Address field. A maximum of 12 host can be entered.

Note In ONS 15600 Software Release 9.0 and later, you can configure an IPv6 address for an FTP server, in addition to an IPv4 address.

Step 6 The Mask is automatically set according to the Net/Subnet Mask length specified in "DLP-E30 Provision IP Settings" task on page 16-37. To change the Mask, click the Up/Down arrows on the **Length** menu.

Step 7 Check the **FTP Relay Enable** radio button to allow FTP commands at the GNE relay. If you will enable the relay at a later time, go to Step 9. Certain TL1 commands executed on an ENE require FTP access into the Data Communication Network (DCN), the FTP relay on the GNE provides this access. The FTP hosts that you have configured in CTC can be used with the TL1 COPY-RFILE (for database backup and restore or software download) or COPY-IOSCFG (for Cisco IOS Configuration File backup and restore) commands.

Step 8 Enter the time, in minutes, that FTP Relay will be enabled. A valid entry is a number between 0 and 60. The number 0 disallows FTP command relay. After the specified time has elapsed the FTP Relay Enable flag is unset and FTP command relay is disallowed.

Step 9 Click OK.

Step 10 Repeat Step 4 through Step 9 to provision additional FTP Hosts.

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

NTP-E24 Set Up Timing

Purpose	This procedure provisions the ONS 15600 timing.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 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-E26 Log into CTC" task on page 16-31 at the node where you want to set up timing. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-E33 Set Up External or Line Timing" task on page 16-43 if an external 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-E34 Set Up Internal Timing" task on page 16-45. This task can only provide Stratum 3E timing.

Note For information about SONET timing, refer to the *Cisco ONS 15600 Reference Manual* or to Telcordia GR-253-CORE.

Stop. You have completed this procedure.

NTP-E26 Create a 1+1 Protection Group

Purpose	This procedure creates a 1+1 protection group. A 1+1 protection group pairs a working OC-N port with a protect OC-N port. The ports on cards can be either working or protect. You can mix working and protect ports on the same card: any OC-192 port can protect another OC-192 port, and any OC-48 port can protect another OC-48 port. You cannot mix OC-192 and OC-48 ports in protection schemes.
Tools/Equipment	None
Prerequisite Procedures	NTP-E11 Install the OC-N Cards, page 2-4 or NTP-E183 Install the ASAP Card, page 2-6 or NTP-E13 Preprovision a Card Slot, page 2-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

Step 2 Verify that the OC-N or ASAP cards are installed.

Step 3 If the optical ports at the source and/or destination nodes are Any Service Any Port (ASAP) pluggable port module (PPM) ports, complete the "NTP-E155 Manage Pluggable Port Modules on the ASAP Card" procedure on page 10-1 and set the port type to OC3, OC12, OC48, or OC192, as necessary.

Step 4 Click the **Provisioning** > **Protection** tabs.

Step 5 Click **Create**.

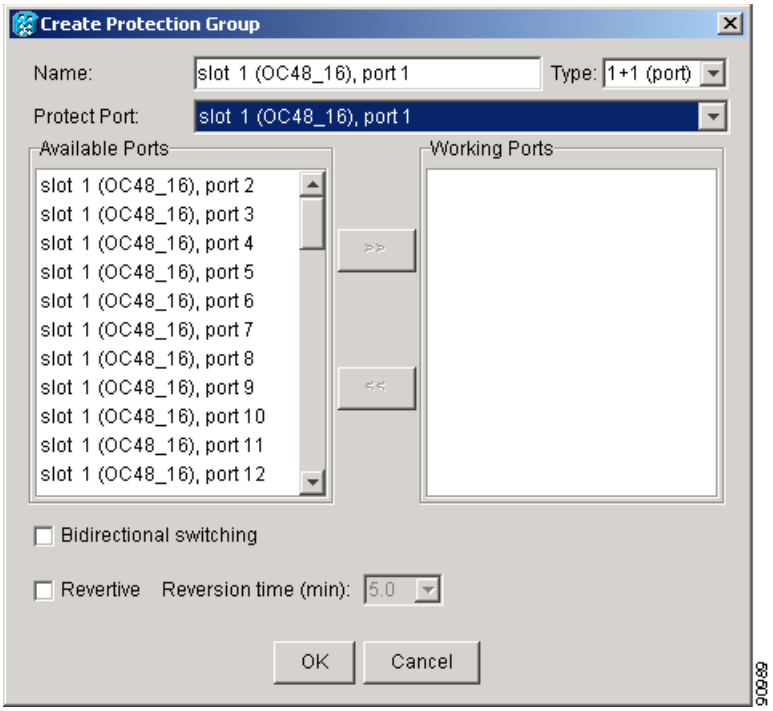
Step 6 In the Create Protection Group dialog box, enter the following:

- Name—Enter 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 (port)** from the drop-down list.

- Protect (Entity) Port—Choose the protect port from the drop-down list. When you choose 1+1 (port) from the Type drop-down list, this field changes from Protect Entity to Protect Port. The list displays the available OC-N ports (Figure 4-3). If OC-N or ASAP cards are not installed, no ports appear in the drop-down list.

After you choose the protect port, a list of working ports available for protection appears in the Available Ports list. If no cards are available, no ports appear. If this occurs, you cannot complete this task until you install the physical cards or preprovision the ONS 15600 slots using the "NTP-E13 Preprovision a Card Slot" procedure on page 2-8.

Figure 4-3 Creating a 1+1 Protection Group



Step 7 From the Available Ports list, choose the working port that will be protected by the port chosen in the Protect Port field. Click the top arrow button to move each port to the Working Ports list.

Step 8 Complete the remaining fields:

- Bidirectional switching—If checked, both the near-end and far-end nodes switch to the designated protection ports. For example, if the near-end node has a loss of signal (LOS) alarm, it switches to the protection port and transmits a switch request to the far-end node to switch to the protection port also. This ensures that both nodes process traffic from the same span.

  If the Bidirectional switching check box is not checked, the near-end and far-end nodes switch independently of each other. For example, if the near-end node has an LOS on its working port it switches to the protection port. If the far-end node does not have a LOS, traffic remains on the working port.

- Revertive—Check this check box if you want traffic to revert to the working port after failure conditions stay corrected for the amount of time entered in the Reversion time field.

- Reversion time—If Revertive is checked, click the Reversion time field and choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the interval between the point when the fault is cleared and the point when the traffic switches to the working port. The reversion timer starts after conditions causing the switch are cleared.

Step 9 Click **OK**.

Stop. You have completed this procedure.

NTP-E27 Set Up SNMP

Purpose	This procedure sets up SNMP parameters so that you can use SNMP management software with the ONS 15600.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 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-E26 Log into CTC" task on page 16-31 at the node where you want to set up SNMP. If you are already logged in, continue with Step 2.

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

Step 3 In the Trap Destinations area, click **Create**.

Step 4 In the Create SNMP Traps Destination dialog box, complete the following:

- IP Address—Enter the IP address of your network management system (NMS). If the node you are logged into is an ENE, set the destination address to the GNE.

  Note In ONS 15600 Software R9.0 and later, you can configure IPv6 addresses for SNMPv1/v2/v3 trap destinations, Get/Set requests and proxy targets, in addition to IPv4 addresses.

- Community—Enter the SNMP community name.

  Note The community name is a form of authentication and access control. The community name assigned to the ONS 15600 is case-sensitive and must match the community name of the NMS. For a description of SNMP community names, refer to the "SNMP" chapter in the *Cisco ONS 15600 Reference Manual*.

- UDP Port—The default User Datagram Protocol (UDP) port for SNMP is 162.
- Trap Version—Choose either SNMPv1 or SNMPv2 from the drop-down list. Refer to your NMS documentation to determine whether to use SNMP v1 or v2.

Step 5 Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.

Step 6 Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears under Selected Destination.

Stop. You have completed this procedure.

NTP-E28 Set the User Code for Card Inventory

Purpose	This procedure creates a user code to help identify the SSXC, TSC, and optical (traffic) cards. The user code is stored in nonvolatile memory on the card so it is not lost when a card is moved or stored as a spare.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31. If you are already logged in, continue with Step 2.

Step 2 Click the **Inventory** tab.

Step 3 In the User Code field, type the code you want to use to identify the card. The user code is a 20-character ASCII string.

Step 4 Click **Apply**.

Stop. You have completed this procedure.

NTP-E29 Configure a Node Using an Existing Database

Purpose	This procedure downloads the provisioning database file from one node to a designated node and assigns a new IP address to the designated node. You can use this procedure to turn up a node or to reconfigure a node.
Tools/Equipment	Database backup file
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Only the provisioning database is downloaded from the specified database backup even if the alarm, performance, or audit logs are included in the database backup.

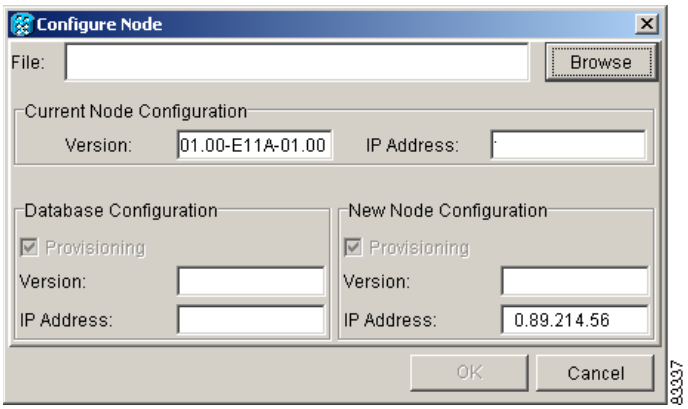
Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31 at the node that you want to configure. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "NTP-E69 Back Up the Database" procedure on page 14-4 to back up the logged in node before reconfiguration.

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

Step 4 Click **Configure**. The Configure Node dialog box appears (Figure 4-4). In the Current Node Configuration area, the Version field displays the current software version.

Figure 4-4 Configuring a Node with Another Node's Database Backup



Step 5 Click **Browse** and navigate to the database backup file you will use to configure the node.

Step 6 In the Database Configuration area, verify the following:

- Provisioning—(Display only) Automatically checked to download the provisioning data from the selected database file.
- Version—(Display only) Displays the software version of the selected database file.
- IP address—(Display only) Displays the IP address assigned to the node of the selected database file.

Step 7 In the New Node Configuration area, verify the following:

- Provisioning—(Display only) Downloads the provisioning data from the selected database file.
- Version—(Display only) Displays the current software version.
- IP address—Displays the current IP address. To assign a new IP address, type a new IP address in the field.

Step 8 Click **OK**. When the Node Configuration warning message appears, click **Yes** to continue. The database restoration window appears. The CTC session closes when the TSC reboots.

Step 9 After the TSC completes its reboot, log in to the node using the IP address assigned in Step 7. For login instructions, see the "DLP-E26 Log into CTC" task on page 16-31.

Stop. You have completed this procedure.

NTP-E48 Set External Alarms and Controls

Purpose	This procedure provisions the reporting parameters and/or virtual wires for external alarms and controls (environmental alarms) that are wired to the Customer Access Panel (CAP or CAP2) alarm contacts.
Tools/Equipment	None
Prerequisite Procedures	DLP-E279 Install Alarm Wires on the CAP/CAP2, page 18-95
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-E53 Provision External Alarms and Virtual Wires" task on page 16-63 to set external alarm inputs.

Step 3 Complete the "DLP-E54 Provision External Controls for External Alarms and Virtual Wires" task on page 16-64 to set external control outputs.

Stop. You have completed this procedure.

NTP-E174 Provision OSI

Purpose	This procedure provisions the ONS 15600 so it can be networked with other vendor NEs that use the Open Systems Interface (OSI) protocol stack for DCN communications. This procedure provisions the TARP, OSI routers, manual area addresses, subnetwork points of attachment, and IP over OSI tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution This procedure requires knowledge of OSI protocols, parameters, and functions. Before you begin, review the OSI sections in the "Management Network Connectivity" chapter in the *Cisco ONS 15600 Reference Manual*.

Caution Do not begin this procedure until you know the role of the ONS 15600 within the OSI and IP network.

Note This procedure requires you to provision non-ONS equipment including routers and third-party NEs. Do not begin until you have the capability to complete that provisioning.

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31 at the node where you want to provision OSI. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the following tasks:

- DLP-E247 Provision OSI Routing Mode, page 18-61—Complete this task first.
- DLP-E248 Provision or Modify TARP Operating Parameters, page 18-62—Complete this task next.
- DLP-E249 Add a Static TID-to-NSAP Entry to the TARP Data Cache, page 18-64—Complete this task as needed.
- DLP-E251 Add a TARP Manual Adjacency Table Entry, page 18-65—Complete this task as needed.
- DLP-E252 Provision OSI Routers, page 18-66—Complete this task as needed.
- DLP-E253 Provision Additional Manual Area Addresses, page 18-67—Complete this task as needed.
- DLP-E254 Enable the OSI Subnet on the LAN Interface, page 18-67—Complete this task as needed.
- DLP-E255 Create an IP-Over-CLNS Tunnel, page 18-68—Complete this task as needed.

Stop. You have completed this procedure.

NTP-E200 Provision Node for SNMPv3

Purpose	This procedure provisions the node to allow SNMPv3 access.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 In node view, click the **Provisioning > SNMP > SNMP V3** tabs.

Step 3 Complete the following tasks as required:

- DLP-E295 Create an SNMPv3 User, page 18-119
- DLP-E296 Create Group Access, page 18-121

Note A group named default_group is defined in the initial configuration. The default group has read and notify access to the complete MIB tree.

- DLP-E295 Create MIB Views, page 18-120

Note A view named full_view is defined in the initial configuration. It includes the complete MIB tree supported on the node.

Stop. You have completed this procedure.

NTP-E201 Provision Node to Send SNMPv3 Traps

Purpose	This procedure provisions a node to send SNMP v3 traps.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 In node view, click the **Provisioning > SNMP > SNMP V3** tabs.

Step 3 Complete the following tasks as required:

- DLP-E295 Create an SNMPv3 User, page 18-119
- DLP-E296 Create Group Access, page 18-121
- DLP-E295 Create MIB Views, page 18-120
- DLP-E299 Create Notification Filters, page 18-123
- DLP-E297 Configure SNMPv3 Trap Destination, page 18-122. When you configure an SNMPv3 trap destination, use the IP address of the NMS, and the port number on which the NMS is listening for traps.

Stop. You have completed this procedure.

NTP-E202 Manually Provision a GNE/ENE to Manage an ENE using SNMPv3

Purpose	This procedure describes how to manually configure a GNE/ENE to allow the NMS to manage an ENE using SNMPv3.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to network view.

Step 3 Double-click the ENE.

Step 4 Click **Provisioning > SNMP > SNMP V3 > General** and note the context engine ID. The context engine ID is required in Step 8.

Step 5 Double-click the GNE.

Step 6 Complete the "DLP-E295 Create an SNMPv3 User" task on page 18-119 to create an SNMPv3 user on the GNE.

Step 7 Complete the following tasks as needed on the ENE:

- DLP-E295 Create an SNMPv3 User, page 18-119
- DLP-E296 Create Group Access, page 18-121
- DLP-E295 Create MIB Views, page 18-120

Step 8 Complete the "DLP-E300 Manually Configure the SNMPv3 Proxy Forwarder Table" task on page 18-124. Use the context engine ID from Step 4, the local user details created in Step 6, and the remote user created in Step 7.

Stop. You have completed this procedure.

NTP-E203 Automatically Provision a GNE to Manage an ENE using SNMPv3

Purpose	This procedure describes how to automatically configure a GNE to allow an NMS to manage an ENE using SNMPv3.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to network view.

Step 3 Double-click the GNE.

Step 4 Complete the DLP-E295 Create an SNMPv3 User, page 18-119to create an SNMPv3 user on the GNE.

Step 5 Complete the "DLP-E301 Automatically Configure the SNMPv3 Proxy Forwarder Table" task on page 19-1. Use the GNE user that you defined in Step 4 when you configure the Proxy Forwarder table.

Note When you use the automatic procedure, CTC automatically creates an ons_proxy user on the ENE, provides ENE user details for the proxy configuration, and provides the context engine ID of the ENE.

Stop. You have completed this procedure.

NTP-E204 Manually Provision a GNE/ENE to Send SNMPv3 Traps from an ENE using SNMPv3

Purpose	This procedure describes how to manually configure the GNE/ENE to allow an ENE to send SNMPv3 traps to the NMS.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to network view.

Step 3 Double-click the GNE.

Step 4 Complete the "DLP-E295 Create an SNMPv3 User" task on page 18-119 to create an SNMPv3 user on the GNE.

Step 5 On the GNE, complete the "DLP-E297 Configure SNMPv3 Trap Destination" task on page 18-122. The target IP address must be the IPv4 or IPv6 address of the NMS. For the UDP Port number, use the port number on which the NMS is listening for traps. Use the user name configured in Step 4. Also, specify a target tag name.

Step 6 Double-click the ENE.

Step 7 Complete the "DLP-E295 Create an SNMPv3 User" task on page 18-119 to create an SNMPv3 user on the ENE.

Step 8 Complete the following tasks as required:

- DLP-E296 Create Group Access, page 18-121 to create a group on the ENE
- DLP-E295 Create MIB Views, page 18-120to create a MIB view on the ENE
- DLP-E299 Create Notification Filters, page 18-123

Step 9 On the ENE, complete the "DLP-E297 Configure SNMPv3 Trap Destination" task on page 18-122. The target IP address should be the IP address of the GNE. The UDP port number is 161. Use the user name configured in Step 7.

Step 10 From the network view, click the **Provisioning > SNMPv3** tabs.

Step 11 Complete the "DLP-E302 Manually Configure the SNMPv3 Proxy Trap Forwarder Table" task on page 19-2.

The source of the trap must be the IP address of the ENE. For the context engine ID field, provide the context engine ID of the ENE. Also, you need to specify the target tag defined in Step 5, and the incoming user details configured in Step 7.

Stop. You have completed this procedure.

NTP-E205 Automatically Provision a GNE/ENE to Send SNMPv3 Traps from an ENE Using SNMPv3

Purpose	This procedure describes how to automatically configure the GNE/ENE to allow an ENE to send SNMPv3 traps to the NMS.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-E26 Log into CTC" task on page 16-31 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to Network View.

Step 3 Double-click the GNE.

Step 4 Complete the task "DLP-E295 Create an SNMPv3 User" task on page 18-119 to create an SNMPv3 user on the GNE.

Step 5 On the GNE, complete the following tasks:

- DLP-E297 Configure SNMPv3 Trap Destination, page 18-122. The target IP address must be the IPv4 or IPv6 address of the NMS. For the UDP Port number, use the port number on which the NMS is listening for traps. Also, specify a target tag name.
- DLP-E302 Automatically Configure the SNMPv3 Proxy Trap Forwarder Table, page 19-3. Use the target tag configured in Step 4. Use the IP address of the ENE as the source of trap. The following details are created automatically:
  - A user named ons_trap_user on the ENE
  - Trap destination on the ENE with an IP address of the GNE as the target IP and 161 as the UDP port number
  - Remote user details of the ENE on the GNE

Stop. You have completed this procedure.