CHAPTER 3

Turn Up a Node

This chapter explains how to provision a single Cisco ONS 15310-MA SDH node and turn it up for service.

Before You Begin

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

- Chapter 1, "Install the Cisco ONS 15310-MA SDH"
- Chapter 2, "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-H148 Verify Card and SFP Installation, page 3-2—Complete this procedure first for the ONS 15310-MA SDH.
2. NTP-H19 Create Users and Assign Security, page 3-3—Complete this procedure to create Cisco Transport Controller (CTC) users and assign their security levels.
3. NTP-H20 Set Up Name, Date, Time, and Contact Information, page 3-3—Continue with this procedure to set the node name, date, time, location, and contact information for a node.
4. NTP-H21 Set Up CTC Network Access, page 3-6— Continue with this procedure to provision the IP address, default router, subnet mask, and network configuration settings including Dynamic Host Configuration Protocol (DHCP), Internet Inter-Orb Protocol (IIOP), proxy server, static routes, Open Shortest Path First (OSPF) protocol, and Routing Information Protocol (RIP).
5. NTP-H177 Set Up the ONS 15310-MA SDH in EMS Secure Access, page 3-6—Continue with this procedure to connect the CTC in secure mode.
6. NTP-H22 Set Up the ONS 15310-MA SDH for Firewall Access, page 3-7—Continue with this procedure if the ONS 15310-MA SDH will be accessed behind firewalls.
7. NTP-H276 Create FTP Host, page 3-8—Continue with this procedure to create FTP host for ENE database backup.
8. NTP-H23 Set Up Timing, page 3-9—Continue with this procedure to set up SDH timing references for the node.
9. NTP-H142 Create Protection Groups for ONS 15310-MA SDH, page 3-10—As needed, complete this procedure to set up protection groups for the ONS 15310-MA SDH.
10. NTP-H25 Set Up SNMP, page 3-12—Complete this procedure if simple network management protocol (SNMP) will be used for network monitoring.

11. NTP-H131 Provision OSI, page 3-13—Complete this procedure if the ONS 15310-MA SDH will be connected to 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.
12. NTP-H180 Provision Node for SNMPv3, page 3-14—Complete this procedure if simple network management protocol (SNMP) will be used for network monitoring

NTP-H148 Verify Card and SFP Installation

Purpose	This procedure verifies that the ONS 15310-MA SDH node is ready for turn up.
Tools/Equipment	An engineering work order, site plan, or other document specifying the ONS 15310-MA SDH card installation
Prerequisite Procedures	Chapter 1, "Install the Cisco ONS 15310-MA SDH"
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 According to your site plan, verify that the 15310E-CTX-K9s are installed.

Step 2 Verify that the green ACT (active) LED is illuminated on one 15310E-CTX-K9 and the amber STBY (standby) LED is illuminated on the second 15310E-CTX-K9, if present.

Note If the 15310E-CTX-K9 cards are not installed, or if their LEDs are not illuminated as described, do not proceed. Repeat the "NTP-H153 Install the 15310E-CTX-K9 Cards" procedure on page 1-16, or refer to the *Cisco ONS 15310-MA SDH Troubleshooting Guide* to resolve installation problems before proceeding to the next step.

Step 3 If you installed an electrical card, verify that it displays a solid green ACT (active) LED on the card faceplate. As necessary, complete the "NTP-H155 Install the Electrical Cards" procedure on page 1-23.

Step 4 If you installed an electrical card, verify that the electrical cables are installed. As necessary, complete the "NTP-H158 Install the Electrical Cables" procedure on page 1-26.

Step 5 If you installed an Ethernet card, verify that it displays a solid green ACT (active) LED. To perform Ethernet card installation, complete the "NTP-H154 Install the Ethernet Cards" procedure on page 1-19.

Step 6 To install a small-form factor pluggable (SFP) connector for the ONS 15310-MA SDH, complete the "DLP-H16 Install SFP Connectors" task on page 16-21. To remove an SFP, complete the "DLP-H17 Remove SFP Connectors" task on page 16-22.

Step 7 Verify that fiber-optic cables are installed and connected to the locations indicated in the site plan. If the fiber-optic cables are not installed, complete the "NTP-H160 Install Optical Cables" procedure on page 1-28 for the ONS 15310-MA SDH.

Step 8 Verify that fiber is routed correctly in the shelf assembly.

Step 9 Continue with the "NTP-H20 Set Up Name, Date, Time, and Contact Information" procedure on page 3-3.

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

NTP-H19 Create Users and Assign Security

Purpose	This procedure creates ONS 15310-MA SDH users and assigns their security levels.
Tools/Equipment	None
Prerequisite Procedures	NTP-H148 Verify Card and SFP Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-H29 Log into CTC" task on page 16-43 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 15310-MA SDH can be used to set up other ONS 15310 users. You can add up to 500 users to one ONS 15310.

Step 2 Complete the "DLP-H37 Create a New User on a Single Node" task on page 16-51 or the "DLP-H38 Create a New User on Multiple Nodes" task on page 16-52 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, complete the "NTP-H83 Modify Users and Change Security" procedure on page 10-6.

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

NTP-H20 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-H148 Verify Card and SFP Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-H29 Log into CTC" task on page 16-43 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—Type a name for the node. For TL1 compliance, names must begin with an alpha character and have no more than 20 alphanumeric characters.
- Contact—Type the name of the node contact person and the contact 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 the desired location. To create a network map that is visible to all ONS 15310-MA SDH users, complete the "NTP-H35 Create a Logical Network Map" procedure on page 4-22. This procedure requires a Superuser security level.

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—Type a description of the node. The description can have 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 15310-MA SDH 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-H75 Display Alarms and Conditions Using Time Zone" task on page 16-93.

  Note Using an NTP or SNTP server ensures that all ONS 15310-MA SDH 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 15310-MA SDH
  - Another ONS 15310-MA SDH with NTP/SNTP enabled that is connected to the ONS 15310-MA SDH

  If you check the gateway network element (GNE) for the ONS 15310-MA SDH proxy server, end ONS 15310 network elements (ENEs) must reference the gateway ONS 15310 for NTP/SNTP timing. For more information about the proxy server feature, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15310-MA SDH Reference Manual*.

  Note In ONS 15310 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 15310-MA SDH for the NTP/SNTP server, make sure the second ONS 15310 references an NTP/SNTP server and not the first ONS 15310 (that is, do not create an NTP/SNTP timing loop by having two ONS 15310s reference each other).

- Date—If the Use NTP/SNTP Server check box is not checked, type the current date in the format mm/dd/yyyy, for example, September 24, 2004 is 09/24/2004.
- Time—If the Use NTP/SNTP Server check box is not checked, type the current time in the format hh:mm:ss, for example, 11:24:58. The ONS 15310-MA SDH 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 list. 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.

Note The ONS 15310-MA SDH clock is not running on battery backup, if power is lost the date and time must be reset.

- Insert AIS-V on VC4 SD-P—Check this check box if you want AIS-Vs inserted on VC low-order path circuits carried byVC3s when the VC3 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 VC3 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 list.

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 to 5 to enter the corrections. If the information is correct, continue with the "NTP-H21 Set Up CTC Network Access" procedure on page 3-6.

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

NTP-H21 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, Routing Information Protocol (RIP), and designated SOCKS servers.
Tools/Equipment	None
Prerequisite Procedures	NTP-H148 Verify Card and SFP Installation, page 3-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-H29 Log into CTC" task on page 16-43. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-H39 Provision IP Settings" task on page 16-53 to provision the ONS 15310-MA SDH IP address, subnet mask, default router, DHCP server, IIOP listener port, and proxy server settings.

Step 3 If static routes are needed, complete the "DLP-H40 Create a Static Route" task on page 16-56. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15310-MA SDH Reference Manual* for further information about static routes.

Step 4 If the ONS 15310-MA SDH 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-H41 Set Up or Change Open Shortest Path First Protocol" task on page 16-57.

Step 5 If the ONS 15310-MA SDH is connected to a LAN or WAN that uses RIP, complete the "DLP-H42 Set Up or Change Routing Information Protocol" task on page 16-59.

Step 6 Complete the "DLP-H274 Provision the Designated SOCKS Servers" task on page 18-75 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-H177 Set Up the ONS 15310-MA SDH in EMS Secure Access

Purpose	This procedure provisions ONS 15310-MA SDH and CTC computers for secure access.
Tools/Equipment	None
Prerequisite Procedures	NTP-H21 Set Up CTC Network Access, page 3-6
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-H22 Set Up the ONS 15310-MA SDH for Firewall Access

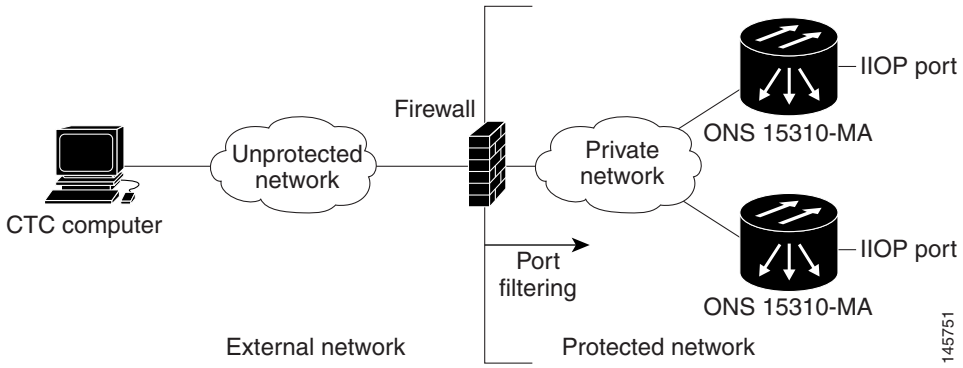
Purpose	This procedure provisions ONS 15310-MA SDH nodes and CTC computers for access through firewalls. If an ONS 15310 or CTC computer resides behind a firewall that uses port filtering, you must enable an Internet Inter-ORB Protocol (IIOP) port on the ONS 15310 SDH and/or CTC computer, depending on whether one or both devices reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	NTP-H148 Verify Card and SFP Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-H29 Log into CTC" task on page 16-43 at a node that is behind the firewall. If you are already logged in, continue with Step 2.

Step 2 If the ONS 15310-MA SDH node resides behind a firewall, complete the "DLP-H43 Provision the IIOP Listener Port on ONS 15310-MA SDH" task on page 16-60.

Figure 3-1 shows an ONS 15310-MA SDH in a protected network and the CTC computer in an external network. For the computer to access the ONS 15310-MA SDH nodes, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15310-MA SDH.

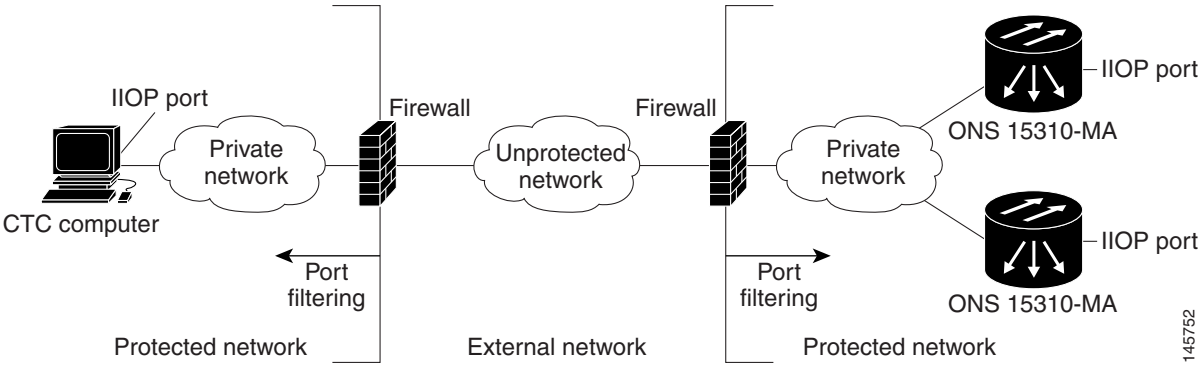
Figure 3-1 ONS 15310-MA SDH Nodes Residing Behind a Firewall



Step 3 If the CTC computer resides behind a firewall, complete the "DLP-H44 Provision the IIOP Listener Port on the CTC Computer" task on page 16-61.

Figure 3-2 shows a CTC computer and ONS 15310-MA SDH behind firewalls. For the computer to access the ONS 15310-MA SDH, you must provision the IIOP port on the CTC computer and on the ONS 15310-MA SDH.

Figure 3-2 CTC Computer and ONS 15310-MA SDHs Residing Behind Firewalls



Stop. You have completed this procedure.

NTP-H276 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-H21 Set Up CTC Network Access, page 3-6 NTP-H22 Set Up the ONS 15310-MA SDH for Firewall Access, page 3-7
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-H29 Log into CTC" task on page 16-43 at the ONS 15310-MA SDH node where you want to set up timing. If you are already logged in, continue with Step 2.

Step 2 In Node view, click the **Provisioning > Network > FTP Hosts** tabs.

Step 3 Click **Create**.

Step 4 Enter a valid IP address in the FTP Host Address field. A maximum of 12 host can be entered.

Note In ONS 15310 Software Release 9.0 and later, you can configure an IPv6 address for an FTP server, in addition to an IPv4 address.

Step 5 The Mask is automatically set according to the Net/Subnet Mask length specified in DLP-C39. To change the Mask, click the Up/Down arrows on the **Length** menu.

Step 6 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 8. 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 CiscoIOS Configuration File backup and restore) commands.

Step 7 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 8 Click OK.

Step 9 Repeat Step 3 through Step 8 to provision additional FTP hosts.

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

NTP-H23 Set Up Timing

Purpose	This procedure provisions the ONS 15310-MA SDH timing.
Tools/Equipment	None
Prerequisite Procedures	NTP-H148 Verify Card and SFP Installation, page 3-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-H29 Log into CTC" task on page 16-43 at the ONS 15310-MA SDH node where you want to set up timing. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-H45 Set Up External or Line Timing" task on page 16-61 if an external building integrated timing supply (BITS) source is available. This is the most common SDH timing setup procedure.

Step 3 Complete the "DLP-H46 Set Up Internal Timing" task on page 16-64 if you cannot complete Step 2 (an external BITS source is not available). This task can only provide Stratum 3 timing.

Note For information about SDH timing, refer to the *Cisco ONS 15310-MA SDH Reference Manual* or to Telcordia GR-253-CORE.

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

NTP-H142 Create Protection Groups for ONS 15310-MA SDH

Purpose	This procedure creates ONS 15310-MA SDH card protection groups.
Tools/Equipment	None
Prerequisite Procedures	NTP-H130 Manage Pluggable Port Modules, page 9-3 (optional) NTP-H148 Verify Card and SFP Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-H29 Log into CTC" task on page 16-43 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

Table 3-1 describes the protection types available on the ONS 15310-MA SDH.

Table 3-1 Protection Types

Type	Cards	Description and Installation Requirements
1:1	E1_21_E3_DS3_3 E1_63_E3_DS3_3	Pairs one working card with one protect card. 1:1 protection groups are created automatically and do not require provisioning. There are two sets of paired expansion slots for the electrical cards. Card slots 1 and 2 are a pair and slots 5 and 6 are a pair. The pairing is due to the configuration of the backplane connectors. When two electrical cards are plugged into either of the card slot pairs, a 1:1 protection group is automatically created for the two cards, if possible. If a protection group cannot be created, one of the cards goes into the Mismatched Equipment Alarm (mismatchofEquipment) state, because the 15310-MA SDH cannot support two unprotected electrical cards in the 1–2 or 5–6 card slot pairs. The 1:1 automatic protection group is created when the second electrical card of a pair is either plugged in or is preprovisioned. All ONS 15310-MA SDH electrical cards, by default, are made part of a 1:1 protection group. The 1:1 protection group cannot be deleted. For more information, refer to the "Card Protection" chapter and the card reference material specific to the card in the *Cisco ONS 15310-MA SDH Reference Manual*.
1+1	15310E-CTX-K9	Pairs a working STM-M port with a protect STM-M port. 1+1 protection can be created between any of the four total optical ports in any combination. For example, 1+1 can created between two ports on the same CTX 2500 card, or it can be created between port 2-1 on one 15310E-CTX-K9 and port 1-1 on the second CTX 2500. You can create a maximum of two 1+1 protection groups, one with the working port on slot 3 and one with the working port on slot 4. The same card can have both working and protect ports on it. 1+1 protection can be revertive or nonrevertive, bidirectional or unidirectional.
Unprotected	Any	Unprotected cards can cause signal loss if a card fails or incurs a signal error. Unprotected is the default for Ethernet cards and for the first electrical card plugged into any of the IO slots. For more information about electrical cards, see 1:1 in this table.

Note The ONS 15310-MA SDH and the 15310E-CTX-K9 card do not support SNCP switching for VC3 circuits containing BIP errors. The SF/SD alarm is not raised for VC3 circuits.

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

- 1:1 protection groups are created automatically when two electrical cards are physically installed or preprovisioned and do not require provisioning.
- "DLP-H242 Create a 1+1 Protection Group for the ONS 15310-MA SDH" task on page 18-47

Note If a protect card is not installed, you can complete the "NTP-H162 Preprovision a Card Slot" procedure on page 1-32 and continue with the card protection provisioning.

Stop. You have completed this procedure.

NTP-H25 Set Up SNMP

Purpose	This procedure provisions the SNMP parameters so that you can use SNMP management software with the ONS 15310-MA SDH.
Tools/Equipment	None
Prerequisite Procedures	NTP-H148 Verify Card and SFP Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-H29 Log into CTC" task on page 16-43 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 In the Trap Destinations area, click **Create**.

Step 4 Complete the following in the Create SNMP Trap Destination dialog box:

- Destination IP Address—Type the IP address of your network management system. If the node you are logged into is an end ONS 15310-MA SDH network element (ENE), set the destination address to the GNE.

Note In ONS 15310 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—Type the SNMP community name. For a description of SNMP community names, refer to the "SNMP" chapter in the *Cisco ONS 15310-MA SDH Reference Manual*.

  Note The community name is a form of authentication and access control. The community name assigned to the ONS 15310-MA SDH 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. (More information about provisioning the UDP port is also given in the "DLP-H225 Set Up SNMP for a GNE" task on page 18-23 and "DLP-H226 Set Up SNMP for an ENE" task on page 18-24.
- Trap Version—Choose either SNMPv1 or SNMPv2. 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 in the Selected Destination list.

Step 7 If you want to set up SNMP remote monitoring (RMON) on GNEs and ENEs, complete the following tasks as required, depending on the protection groups you want to create:

- DLP-H225 Set Up SNMP for a GNE, page 18-23
- DLP-H226 Set Up SNMP for an ENE, page 18-24
- DLP-H227 Format and Enter NMS Community String for SNMP Command or Operation, page 18-26

Step 8 Click **Apply**.

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

NTP-H131 Provision OSI

Purpose	This procedure provisions the ONS 15310-MA SDH so it can be networked with other vendor NEs that use the OSI (Open Systems Interface) protocol stack for data communications network (DCN) communications. This procedure provisions the TID Address Resolution Protocol (TARP), OSI routers, manual area addresses, subnetwork points of attachment, and IP over OSI tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-H148 Verify Card and SFP Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Caution This procedure requires an understanding of OSI protocols, parameters, and functions. Before you begin, review the OSI reference sections in the "Management Network Connectivity" chapter in the *Cisco ONS 15310-MA SDH Reference Manual*.

Caution Do not begin this procedure until you know the role of the ONS 15310-MA SDH within the OSI and IP network.

Note This procedure requires provisioning of 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-H29 Log into CTC, page 16-43 at the node where you want to provision the OSI routing mode. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the following tasks:

- DLP-H200 Provision OSI Routing Mode, page 18-1—Complete this task first.
- DLP-H201 Provision or Modify TARP Operating Parameters, page 18-2—Complete this task next.

- DLP-H202 Add a Static TID to NSAP Entry to the TARP Data Cache, page 18-4—Complete this task as needed.
- DLP-H204 Add a TARP Manual Adjacency Table Entry, page 18-5—Complete this task as needed.
- DLP-H205 Provision OSI Routers, page 18-6—Complete this task as needed.
- DLP-H206 Provision Additional Manual Area Addresses, page 18-6—Complete this task as needed.
- DLP-H207 Enable the OSI Subnet on the LAN Interface, page 18-7—Complete this task as needed.
- DLP-H208 Create an IP-Over-CLNS Tunnel, page 18-8—Complete this task as needed.

Stop. You have completed this procedure.

NTP-H180 Provision Node for SNMPv3

Purpose	This procedure provisions the node to allow SNMPv3 access.
Tools/Equipment	None
Prerequisite Procedures	NTP-H148 Verify Card and SFP Installation, page 3-2
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-H29 Log into CTC" task on page 16-43 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-H282 Create an SNMPv3 User, page 18-83
- DLP-H284 Create Group Access, page 18-84

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-H283 Create MIB Views, page 18-84

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-H181 Provision Node to Send SNMPv3 Traps

Purpose	This procedure provisions a node to send SNMP v3 traps.
Tools/Equipment	None
Prerequisite Procedures	NTP-H148 Verify Card and SFP Installation, page 3-2
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-H29 Log into CTC" task on page 16-43 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-H282 Create an SNMPv3 User, page 18-83
- DLP-H284 Create Group Access, page 18-84
- DLP-H283 Create MIB Views, page 18-84
- DLP-H287 Create Notification Filters, page 18-87
- DLP-H285 Configure SNMPv3 Trap Destination, page 18-85. 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-H182 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-H148 Verify Card and SFP Installation, page 3-2
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-H29 Log into CTC" task on page 16-43 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-H282 Create an SNMPv3 User" task on page 18-83 to create an SNMPv3 user on the GNE.

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

- DLP-H282 Create an SNMPv3 User, page 18-83
- DLP-H284 Create Group Access, page 18-84
- DLP-H283 Create MIB Views, page 18-84

Step 8 Complete the "DLP-H288 Manually Configure the SNMPv3 Proxy Forwarder Table" task on page 18-87. 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-H183 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-H148 Verify Card and SFP Installation, page 3-2
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-H29 Log into CTC" task on page 16-43 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-H282 Create an SNMPv3 User" task on page 18-83 to create an SNMPv3 user on the GNE.

Step 5 Complete the "DLP-H289 Automatically Configure the SNMPv3 Proxy Forwarder Table" task on page 18-88. 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 the context engine ID of the ENE.

Stop. You have completed this procedure.

NTP-H184 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-H148 Verify Card and SFP Installation, page 3-2
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-H29 Log into CTC" task on page 16-43 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-H282 Create an SNMPv3 User" task on page 18-83 to create an SNMPv3 user on the GNE.

Step 5 On the GNE, complete the DLP-H285 Configure SNMPv3 Trap Destination, page 18-85. 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-H282 Create an SNMPv3 User" task on page 18-83 to create an SNMPv3 user on the ENE.

Step 8 Complete the following tasks as required:

- DLP-H284 Create Group Access, page 18-84 to create a group on the ENE
- DLP-H283 Create MIB Views, page 18-84 to create a MIB view on the ENE
- DLP-H287 Create Notification Filters, page 18-87

Step 9 On the ENE, complete the "DLP-H285 Configure SNMPv3 Trap Destination" task on page 18-85. 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-H290 Manually Configure the SNMPv3 Proxy Trap Forwarder Table" task on page 18-89.

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-H185 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-H148 Verify Card and SFP Installation, page 3-2
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-H29 Log into CTC" task on page 16-43 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-H282 Create an SNMPv3 User" task on page 18-83 to create an SNMPv3 user on the GNE.

Step 5 On the GNE, complete the following tasks:

- DLP-H285 Configure SNMPv3 Trap Destination, page 18-85. 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-H291 Automatically Configure the SNMPv3 Proxy Trap Forwarder Table, page 18-90. Use the target tag configured in Step 4. Use the IP address of the ENE as the source of trap. Create trap destination on the ENE with an IP address of the GNE as the target IP and 161 as the UDP port number. The following details are created automatically:
  - A user named ons_trap_user on the ENE
  - Remote user details of the ENE on the GNE

Stop. You have completed this procedure.