CHAPTER 3

# Turn Up a Node

This chapter explains how to provision a single Cisco ONS 15454 SDH 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 Shelf and FMECs”
- Chapter 2, “Install Cards and Fiber-Optic Cable”
- Chapter 4, “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-D24 Verify Card Installation, page 3-2—Complete this procedure first.
2. NTP-D30 Create Users and Assign Security, page 3-4—Continue with this procedure to create Cisco Transport Controller (CTC) users and assign their security levels.
3. NTP-D316 Set Up Name, Date, Time, and Contact Information, page 3-4—Continue with this procedure to set the node name, date, time, location, and contact information.
4. NTP-D279 Set Power Monitor Thresholds, page 3-7—Continue with this procedure to set the node battery power thresholds.
5. NTP-D169 Set Up CTC Network Access, page 3-7—Continue with this procedure to provision the IP address, default router, subnet mask, and network configuration settings.
6. NTP-D364 Set Up the ONS 15454 in Secure Mode, page 3-8—Continue with this procedure to connect the CTC in secure mode.
7. NTP-A360 Enable EMS Secure Access, page 3-9—Continue with this procedure to enable EMS secure access and provide enhanced SFTP and SSH security.
8. NTP-D378 Set Up Secure Access to the ONS 15454 SDH TL1, page 3-9—Continue with this procedure to enable secure access to TL1.
9. NTP-D27 Set Up the ONS 15454 SDH for Firewall Access, page 3-10—Continue with this procedure if the ONS 15454 SDH will be accessed behind firewalls.
10. NTP-D361 Create FTP Host, page 3-11 - Continue with this procedure if to create FTP host for ENE database backup.

11. NTP-D28 Set Up Timing, page 3-12—Continue with this procedure to set up the node's SDH timing references.
12. NTP-D170 Create Protection Groups, page 3-13—Complete this procedure, as needed, to set up 1:1, 1:N, or 1+1 protection groups for ONS 15454 SDH electrical and optical cards.
13. NTP-D171 Set Up SNMP, page 3-15—Complete this procedure if Simple Network Management Protocol (SNMP) will be used for network monitoring.
14. NTP-D368 Provision Node for SNMPv3, page 3-17—Complete this procedure if Simple Network Management Protocol version 3 (SNMPv3) will be used for network monitoring.
15. NTP-D326 Provision OSI, page 3-16—Complete this procedure if the ONS 15454 SDH will be connected in networks with network elements (NEs) that are based on the Open System Interconnection (OSI) protocol stack. This procedure provisions the Target Identifier Address Resolution Protocol (TARP), OSI routers, manual area addresses, subnetwork points of attachment, and IP-over-OSI tunnels.

# NTP-D24 Verify Card Installation

| | |
|---|---|
| **Purpose** | This procedure verifies that the ONS 15454 SDH node is ready for turn-up. |
| **Tools/Equipment** | An engineering work order, site plan, or other document specifying the ONS 15454 SDH card installation. |
| **Prerequisite Procedures** | Chapter 1, "Install the Shelf and FMECs"<br>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/TCC2P cards are installed in Slots 7 and 11.

**Step 2** Verify that the green ACT (active) LED is illuminated on one TCC2/TCC2P card and the amber STBY (standby) LED is illuminated on the second TCC2/TCC2P card.

**Note** If the TCC2/TCC2P cards are not installed, or if their LEDs are not operating as described, do not proceed. Repeat the "DLP-D332 Install the TCC2/TCC2P Cards" task on page 20-23, or refer to the *Cisco ONS 15454 SDH Troubleshooting Guide* to resolve installation problems before proceeding to Step 3.

**Step 3** Verify that cross-connect cards (XC-VXL-2.5G, XC-VXL-10G, XC-VXC-10G) 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 illuminated as described, do not proceed. Repeat the "DLP-D333 Install the XC-VXL-10G, XC-VXL-2.5G, or XC-VXC-10G Cards" task on page 20-26, or refer to the *Cisco ONS 15454 SDH Troubleshooting Guide* to resolve installation problems before proceeding to Step 5.

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

**Step 6** Verify that electrical cards (E1-42, E3-12, DS3i-N-12, or STM1E) are installed in the ONS 15454 SDH slots as designated by your installation plan.

**Step 7** If your site requires an Ethernet card, verify that the Ethernet card (E100T-12, E100T-12-G, E1000-2, E1000-2-G, G1K-4, ML1000-2, ML100T-12, ML-100X-8, CE-1000-4, ML-MR-10, or CE-MR-10) is installed in Slots 1 to 6 or 12 to 17, and that its ACT (active) LED displays a solid green light.

**Step 8** If an E1000-2, E1000-2-G, G1K-4, ML1000-2, ML100X-8, CE-1000-4, ML-MR-10, or CE-MR-10 Ethernet card is installed, verify that it has a Gigabit Interface Converter (GBIC) or Small Form-factor Pluggable (SFP/XFP) installed. If not, see the "DLP-D335 Install GBIC or SFP/XFP Devices" task on page 20-29.

**Step 9** Verify that STM-N cards (STM-1, STM-1-8, STM-4, STM-4-4, STM-16, STM-16 any slot (AS), STM-64, MRC-12, and MRC-2.5G-4) are installed in the slots designated by your site plan. STM-1, STM-4, and STM-16 AS cards can be installed in Slots 1 to 6 or 12 to 17. The STM-1-8 and STM-4-4 can only be installed in Slots 1 to 4 or 14 to 17, and the STM-16 and STM-64 can only be installed in Slots 5 to 6 and 12 to 13.

**Step 10** Verify that all installed STM-N cards display a solid amber STBY LED.

**Step 11** If transponder or muxponder cards are installed (TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, MXPP_MR_2.5G, MXP_2.5G_10G, TXP_MR_10E, TXP_MR_10E_L, TXP_MR_10E_C, MXP_2.5G_10E, MXP_2.5G_10E_C, MXP_2.5G_10E_L, MXP_MR_10DME_L, MXP_MR_10DME_C, ADM-10G, GE_XP, or 10GE_XP), verify that they are installed in Slots 1 to 6 or 12 to 17 and have GBIC or SFP connectors are installed. For information about installing and provisioning TXP and MXP cards, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.

**Step 12** If Fibre Channel (FC_MR-4) cards are installed, verify that the FC_MR-4 card is installed in Slots 1 to 6 or 12 to 17 and displays a solid green ACT (Active) LED.

**Step 13** 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-D19 Install Fiber-Optic Cables on Optical Cards" procedure on page 2-17.

**Step 14** 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-D245 Route Fiber-Optic Cables" procedure on page 2-20. If the fiber boots are not installed, complete the "DLP-D45 Install the Fiber Boot" task on page 17-31.

**Step 15** 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 SDH software CD. Refer to the release-specific software upgrade document for instructions.
- Replace the TCC2/TCC2P cards with cards containing the correct release. Refer to the *Cisco ONS 15454 SDH Troubleshooting Guide*.

**Step 16** Continue with the "NTP-D30 Create Users and Assign Security" procedure on page 3-4.

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

# NTP-D30 Create Users and Assign Security

| | |
|---|---|
| **Purpose** | This procedure creates ONS 15454 SDH users and assigns their security levels. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D24 Verify Card Installation, page 3-2 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser only |

**Step 1** Complete the "DLP-D60 Log into CTC" task on page 17-45 at the node where you want 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 SDH can be used to set up other ONS 15454 SDH users. You can add up to 500 users to one ONS 15454 SDH.

**Step 2** Complete the "DLP-D74 Create a New User on a Single Node" task on page 17-61 or the "DLP-D75 Create a New User on Multiple Nodes" task on page 17-62 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-D205 Modify Users and Change Security" procedure on page 11-7.

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

# NTP-D316 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-D24 Verify Card Installation, page 3-2 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser only |

**Step 1** Complete the "DLP-D60 Log into CTC" task on page 17-45 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—(Optional) Type 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 on the network view map. Press **Ctrl** then drag and drop the node icon. To create a logical network map for all ONS 15454 SDH users, complete the "NTP-D172 Create a Logical Network Map" procedure on page 5-41.

**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 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 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-D112 Display Alarms and Conditions Using Time Zone" task on page 18-15.

  **Note** Using an NTP or SNTP server ensures that all ONS 15454 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, complete the following fields:

  - Use NTP/SNTP Server—Type the IP address of the primary NTP/SNTP server connected to the ONS 15454 SDH or of another ONS 15454/15310-MA/15600 SDH as GNE with NTP/SNTP enabled that is connected to the ONS 15454 SDH ENE.
  - Backup NTP/SNTP Server—Type the IP address of the secondary NTP/SNTP server connected to the ONS 15454 SDH or of another ONS 15454 /15310-MA/15600 SDH as GNE with NTP/SNTP enabled that is connected to the ONS 15454 SDH 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 15454 SDH SOCKS proxy server, (see the "DLP-D249 Provision IP Settings" task on page 19-55), external ONS 15454 SDH nodes must reference the gateway ONS 15454 SDH for NTP/SNTP timing. For more information about the SOCKS proxy server feature, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

**Note** In ONS 15454 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 15454 SDH for the NTP/SNTP server, make sure the second ONS 15454 SDH references an NTP/SNTP server and not the first ONS 15454 SDH (that is, do not create an NTP/SNTP timing loop by having two ONS 15454 SDH nodes reference each other).

- Date—If Use NTP/SNTP Server is not selected, type the current date in the format mm/dd/yyyy, for example, September 24, 2004 is 09/24/2004.
- Time—If Use NTP/SNTP Server is not selected, type the current time in the format hh:mm:ss, for example, 11:24:58. The ONS 15454 SDH uses a 24-hour clock, so 10:00 PM is entered as 22:00:00.

**Note** To change the global date format from American to European, select the appropriate format on the General tab of the CTC Preferences window. American format is mm/dd/yyyy, for example, September 24, 2004 is 09/24/2004. European format is dd/mm/yyyy, for example, September 24, 2004 is 24/09/2004.

- Time Zone—Click the field and choose a city within your time zone from the drop-down list. The list 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 uses Daylight Savings Time.

**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-D279 Set Power Monitor Thresholds" procedure on page 3-7.

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

# NTP-D279 Set Power Monitor Thresholds

| | |
|---|---|
| **Purpose** | This procedure provisions extreme high low, and extreme low input battery power thresholds within a –48 VDC environment. When the thresholds are crossed, the TCC2/TCC2P generates warning alarms in CTC. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D24 Verify Card Installation, page 3-2 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** Complete the "DLP-D60 Log into CTC" task on page 17-45 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 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-D169 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, dual IP address setting, static routes, Open Shortest Path First (OSPF) protocol, Routing Information Protocol (RIP), and designated SOCKS servers. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D24 Verify Card Installation, page 3-2 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser only |

**Step 1** Complete the "DLP-D60 Log into CTC" task on page 17-45. If you are already logged in, continue with Step 2.

**Step 2** Complete the "DLP-D249 Provision IP Settings" task on page 19-55 to provision the ONS 15454 SDH IP address, subnet mask, default router, DHCP, IIOP listener port, and SOCKS proxy server settings.

**Tip** If you cannot log into the node, you might be able to change its IP address, default router, and network mask by using the LCD on the ONS 15454 SDH front panel. See the "DLP-D64 Set the IP Address, Default Router, and Network Mask Using the LCD" task on page 17-50 for instructions. However, you cannot use the LCD to provision any other network settings.

**Step 3** If you want to turn on the ONS 15454 secure mode, which allows two IP addresses to be provisioned for the node if TCC2P cards are installed, complete the "DLP-D84 Enable Node Secure Mode" task on page 17-74. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 SDH Reference Manual* for information about secure mode.

**Step 4** If static routes are needed, complete the "DLP-D65 Create a Static Route" task on page 17-52. Refer to the "CTC Network Connectivity" chapter in the *Cisco ONS 15454 SDH Reference Manual* for further information about static routes.

**Step 5** If the ONS 15454 SDH is connected to a LAN or WAN that uses OSPF and you want to share routing information between the LAN or WAN and the ONS network, complete the "DLP-D250 Set Up or Change Open Shortest Path First Protocol" task on page 19-60.

**Step 6** If the ONS 15454 SDH is connected to a LAN or WAN that uses RIP, complete the "DLP-D251 Set Up or Change Routing Information Protocol" task on page 19-62.

**Step 7** Complete the "DLP-D289 Provision the Designated SOCKS Servers" task on page 19-82 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-D364 Set Up the ONS 15454 in Secure Mode

| | |
|---|---|
| **Purpose** | This procedure provisions ONS 15454s and CTC computers for secure access. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D169 Set Up CTC Network Access, page 3-7 |
| **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-A360 Enable EMS Secure Access

| | |
|---|---|
| **Purpose** | This procedure enables EMS secure access. This procedure enables enhanced SFTP and SSH security. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D169 Set Up CTC Network Access, page 3-7 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Step 1** In shelf 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** Set the listener port value by choosing "Other constant" radio button.

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

# NTP-D378 Set Up Secure Access to the ONS 15454 SDH TL1

| | |
|---|---|
| **Purpose** | This procedure provisions ONS 15454 SDH nodes for secure access to TL1. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D169 Set Up CTC Network Access, page 3-7 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

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

**Step 2** Under the **TL1 Access** area, change the **Access State** to **Secure**.

**Step 3** Click **Apply**.

Existing non-secure TL1 sessions, if any, are terminated.

**Step 4** To create a secure TL1 connection, enter the following command at the UNIX or Linux prompt:

**ssh -l** *username node-ip* **-p** *port-number*

The port number for secure TL1 is 4083.

**Note** Use any SSH client on Windows.

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

# NTP-D27 Set Up the ONS 15454 SDH for Firewall Access

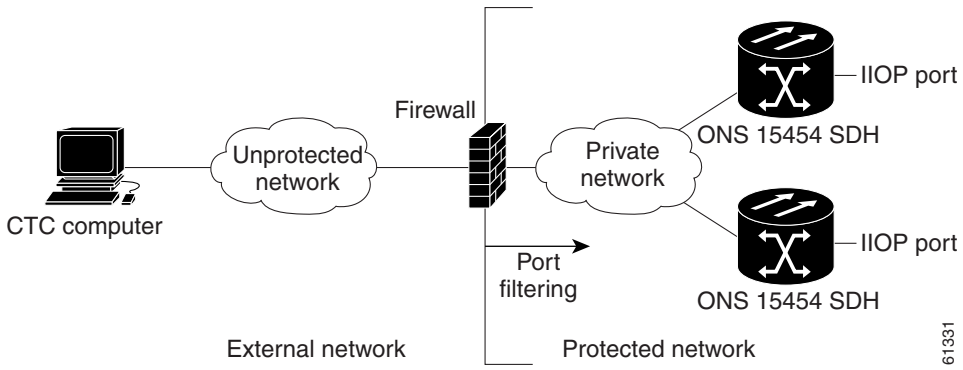
| | |
|---|---|
| **Purpose** | This procedure provisions ONS 15454 SDH nodes and CTC computers for access through firewalls. |
| **Tools/Equipment** | IIOP listener port number provided by your LAN or firewall administrator |
| **Prerequisite Procedures** | NTP-D24 Verify Card Installation, page 3-2 |
| **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-D60 Log into CTC" task on page 17-45 for instructions. If you are already logged in, continue with Step 2.

**Step 2** Complete the "DLP-D67 Provision the IIOP Listener Port on the ONS 15454 SDH" task on page 17-53.

Figure 3-1 shows ONS 15454 SDH nodes in a protected network and the CTC computer in an external network. For the computer to access the ONS 15454 SDH nodes, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15454 SDH.

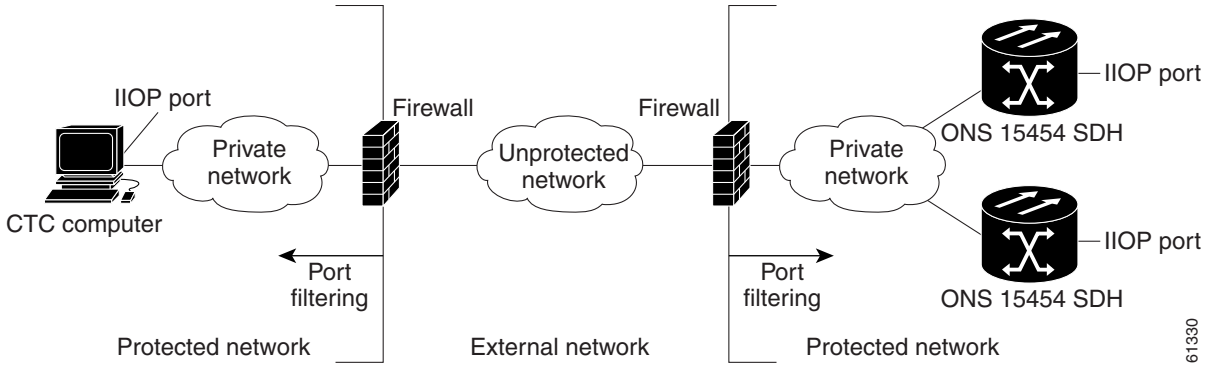
*Figure 3-1 ONS 15454 SDH Nodes Residing Behind a Firewall*



**Step 3** If the CTC computer resides behind a firewall, complete the "DLP-D68 Provision the IIOP Listener Port on the CTC Computer" task on page 17-54.

Figure 3-2 shows a CTC computer and ONS 15454 SDH behind firewalls. For the computer to access the ONS 15454 SDH, you must provision the IIOP port on the CTC computer and on the ONS 15454 SDH. Each firewall can use a different IIOP port.

*Figure 3-2 CTC Computer and ONS 15454 SDH Nodes Residing Behind Firewalls*




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

# NTP-D361 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-D169 Set Up CTC Network Access, page 3-7<br>NTP-D27 Set Up the ONS 15454 SDH for Firewall Access, page 3-10 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Step 1** Complete the "DLP-D60 Log into CTC" task on page 17-45. If you are already logged in, continue with Step 2.

**Step 2** If you want to turn on the ONS 15454 secure mode, which allows two IPv4 addresses to be provisioned for the node if TCC2P cards are installed, complete the "DLP-D84 Enable Node Secure Mode" task on page 17-74. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 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 15454 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-D249 Provision IP Settings" section on page 19-55. 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-D28 Set Up Timing

| | |
|---|---|
| **Purpose** | This procedure provisions the ONS 15454 SDH timing. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D24 Verify Card Installation, page 3-2 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** Complete the "DLP-D60 Log into CTC" task on page 17-45 the ONS 15454 SDH node where you want to set up timing. If you are already logged in, continue with Step 2.

**Step 2** Complete the "DLP-D69 Set Up External or Line Timing" task on page 17-54 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-D70 Set Up Internal Timing" task on page 17-57 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 "Timing" chapter in the *Cisco ONS 15454 SDH Reference Manual* or ITU-T G.784.

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

# NTP-D170 Create Protection Groups

| | |
|---|---|
| **Purpose** | This procedure creates ONS 15454 SDH card protection groups. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D24 Verify Card Installation, page 3-2 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** Complete the "DLP-D60 Log into CTC" task on page 17-45 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 15454 SDH.

*Table 3-1 Card Protection Types*

| Type | Cards | Description and Installation Requirements |
|---|---|---|
| 1:1 | DS3i-N-12<br>E3-12<br>STM1E | 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/TCC2P, 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 and the card reference material specific to the card in the *Cisco ONS 15454 SDH Reference Manual*. |
| 1:N | E1-42N<br>DS3i-N-12 | 1:N protection allows a single card to protect up to five (four for the DS3i-N-12 card) working cards of the same electrical level. An E1-42N card protects E1-42N cards and a DS3i-N-12 card protects DS3i-N-12 cards. For more information, refer to the "Card Protection" chapter and the card reference material specific to the card in the *Cisco ONS 15454 SDH Reference Manual*. |
| 1+1 | Any STM-N | Pairs a working STM-N card/port with a protect STM-N card/port. For multiport STM-N cards, the protect port must match the working port on the working card. For example, Port 1 of an STM-1 card can only be protected by Port 1 of another STM-1 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, unidirectional or bidirecitonal. |

*Table 3-1 Card Protection Types (continued)*

| Type | Cards | Description and Installation Requirements |
|---|---|---|
| Y Cable | TXP_MR_10G<br>TXP_MR_10E<br>TXP_MR_2.5G<br>MXP_2.5G_10G<br>MXP_2.5G_10E<br>MXP_2.5G_10E_C<br>MXP_2.5G_10E_L<br>MXP_MR_2.5G<br>MXP_MR_10DME_C<br>MXP_MR_10DME_L<br>GE_XP (in 10GE or 20GE MXP card mode)<br>10GE_XP (in 10GE TXP card mode) | 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. To provision y-cable protection, see the *Cisco ONS 15454 DWDM Procedure Guide*. |
| Splitter | TXPP_MR_2.5G<br>MXPP_MR_2.5G | Splitter protection is automatically provided with the TXPP_MR_2.5G and MXPP_MR_2.5G cards. For more information, refer to the *Cisco ONS 15454 DWDM Procedure Guide*. |
| 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 SDH. Unprotected is the default protection type. |

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

- DLP-D71 Create a 1:1 Protection Group, page 17-58
- DLP-D72 Create a 1:N Protection Group, page 17-59
- DLP-D73 Create a 1+1 Protection Group, page 17-60

**Note** If a protect card is not installed, you can complete the "DLP-D442 Preprovision a Slot" task on page 21-33 and continue with the card protection provisioning.

**Note** A 1+1 protection group can only be provisioned between the same equipment type, using the same port number, and the same port rate. The MRC- 4 (MRC- 4 to MRC- 4 pairing) or MRC-12 (MRC-12 to MRC-12 pairing) cards can be in the same slot type or in different slot type; one in low speed-slot and one in high-speed slot.

**Note** To provision Y-cable protection for TXP and MXP cards, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.

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

# NTP-D171 Set Up SNMP

| | |
|---|---|
| **Purpose** | This procedure provisions the SNMP parameters so that you can use SNMP management software with the ONS 15454 SDH. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D24 Verify Card Installation, page 3-2 |
| **Required/As Needed** | Required if SNMP is used at your site. |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** Complete the "DLP-D60 Log into CTC" task on page 17-45 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 (Figure 3-3):

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

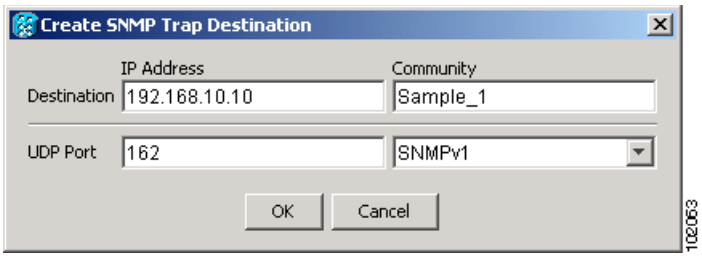
  **Note** In ONS 15454 Software R9.0 and later, you can configure IPv6 addresses for SNMPv1/v2/v3 trap destinations, Get/Set requests and proxy targets, in addition to IPv4 addresses

- Community—Type the SNMP community name. For a description of SNMP community names, refer to the "SNMP" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

  **Note** The community name is a form of authentication and access control. The community name assigned to the ONS 15454 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-D151 Set Up SNMP for a GNE" task on page 18-43 and "DLP-D153 Set Up SNMP for an ENE" task on page 18-46.)
- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMP v1 or v2.

*Figure 3-3 Creating an SNMP Trap Destination*




**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 DLPs as required, depending on the protection groups that you want to create:

- DLP-D151 Set Up SNMP for a GNE, page 18-43
- DLP-D153 Set Up SNMP for an ENE, page 18-46
- DLP-D162 Format and Enter NMS Community String for SNMP Command or Operation, page 18-53

**Step 8** Click **Apply**.

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

# NTP-D326 Provision OSI

| | |
|---|---|
| **Purpose** | This procedure provisions the ONS 15454 SDH so it can be networked with other vendor NEs that use the OSI protocol stack for data communications network (DCN) communications. This procedure provisions the TARP, OSI routers, manual area addresses, subnetwork points of attachment, and IP-over-ConnectionLess Network Service (CLNS) tunnels. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D24 Verify Card Installation, page 3-2 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | Provisioning or higher |

**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 15454 SDH Reference Manual*.

**Caution** Do not begin this procedure until you know the role of the ONS 15454 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-D60 Log into CTC" task on page 17-45 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-D165 Provision OSI Routing Mode, page 18-54—Complete this task first.
- DLP-D166 Provision or Modify TARP Operating Parameters, page 18-56—Complete this task next.
- DLP-D167 Add a Static TID-to-NSAP Entry to the TARP Data Cache, page 18-58—Complete this task as needed.
- DLP-D169 Add a TARP Manual Adjacency Table Entry, page 18-59—Complete this task as needed.
- DLP-D171 Provision OSI Routers, page 18-60—Complete this task as needed.
- DLP-D172 Provision Additional Manual Area Addresses, page 18-61—Complete this task as needed.
- DLP-D173 Enable the OSI Subnet on the LAN Interface, page 18-61—Complete this task as needed.
- DLP-D174 Create an IP-Over-CLNS Tunnel, page 18-62—Complete this task as needed.

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

# NTP-D368 Provision Node for SNMPv3

| | |
|---|---|
| **Purpose** | This procedure provisions the node to allow SNMPv3 access. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D24 Verify Card 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-D60 Log into CTC" task on page 17-45 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-D483 Create an SNMPv3 User, page 21-58
- DLP-D485 Create Group Access, page 21-60

**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-D484 Create MIB Views, page 21-59

**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-D369 Provision Node to Send SNMPv3 Traps

| | |
|---|---|
| **Purpose** | This procedure provisions a node to send SNMP v3 traps. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-D24 Verify Card 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-D60 Log into CTC" task on page 17-45 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-D483 Create an SNMPv3 User, page 21-58
- DLP-D485 Create Group Access, page 21-60
- DLP-D484 Create MIB Views, page 21-59
- DLP-D488 Create Notification Filters, page 21-62
- DLP-D486 Configure SNMPv3 Trap Destination, page 21-61. 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-D370 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-D24 Verify Card 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-D60 Log into CTC" task on page 17-45 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-D483 Create an SNMPv3 User" task on page 21-58 to create an SNMPv3 user on the GNE.

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

- DLP-D483 Create an SNMPv3 User, page 21-58
- DLP-D485 Create Group Access, page 21-60
- DLP-D484 Create MIB Views, page 21-59

**Step 8** Complete the "DLP-D489 Manually Configure the SNMPv3 Proxy Forwarder Table" task on page 21-63. 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-D371 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-D24 Verify Card 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-D60 Log into CTC" task on page 17-45 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-D483 Create an SNMPv3 User" task on page 21-58 to create an SNMPv3 user on the GNE.

**Step 5** Complete the "DLP-D490 Automatically Configure the SNMPv3 Proxy Forwarder Table" task on page 21-64. 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-D372 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-D24 Verify Card 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-D60 Log into CTC" task on page 17-45 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-D483 Create an SNMPv3 User" task on page 21-58 to create an SNMPv3 user on the GNE.

**Step 5** On the GNE, complete the "DLP-D486 Configure SNMPv3 Trap Destination" task on page 21-61. 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-D483 Create an SNMPv3 User" task on page 21-58 to create an SNMPv3 user on the ENE.

**Step 8** Complete the following tasks as required:

- DLP-D485 Create Group Access, page 21-60 to create a group on the ENE
- DLP-D484 Create MIB Views, page 21-59 to create a MIB view on the ENE
- DLP-D488 Create Notification Filters, page 21-62

**Step 9** On the ENE, complete the "DLP-D486 Configure SNMPv3 Trap Destination" task on page 21-61. 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-D491 Manually Configure the SNMPv3 Proxy Trap Forwarder Table" task on page 21-65.

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-D373 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-D24 Verify Card 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-D60 Log into CTC" task on page 17-45 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-D483 Create an SNMPv3 User" task on page 21-58 to create an SNMPv3 user on the GNE.

**Step 5** On the GNE, complete the following tasks:

- DLP-D486 Configure SNMPv3 Trap Destination, page 21-61. 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-D492 Automatically Configure the SNMPv3 Proxy Trap Forwarder Table, page 21-66. 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.**