



# CHAPTER 4

## Turn Up a Node

---

This chapter explains how to provision a single Cisco ONS 15310-CL or Cisco ONS 15310-MA 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-CL”](#)
- [Chapter 2, “Install the Cisco ONS 15310-MA”](#)
- [Chapter 3, “Connect the PC and Log into the GUI”](#)

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

1. [NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2](#)—Complete this procedure first for the ONS 15310-CL.
2. [NTP-C148 Verify Card and SFP Installation for the ONS 15310-MA, page 4-3](#)—Complete this procedure first for the ONS 15310-MA.
3. [NTP-C19 Create Users and Assign Security, page 4-4](#)—Complete this procedure to create Cisco Transport Controller (CTC) users and assign their security levels.
4. [NTP-C20 Set Up Name, Date, Time, and Contact Information, page 4-4](#)—Continue with this procedure to set the node name, date, time, location, and contact information for a node.
5. [NTP-C21 Set Up CTC Network Access, page 4-6](#)—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).
6. [NTP-C177 Set Up the ONS 15310 in EMS Secure Access, page 4-7](#)—Continue with this procedure to connect the CTC in secure mode.
7. [NTP-C22 Set Up the ONS 15310-CL or ONS 15310-MA for Firewall Access, page 4-8](#)—Continue with this procedure if the ONS 15310-CL or ONS 15310-MA will be accessed behind firewalls.
8. [NTP-C276 Create FTP Host, page 4-10](#)—Continue with this procedure to create FTP host for ENE database backup.
9. [NTP-C23 Set Up Timing, page 4-11](#)—Continue with this procedure to set up SONET timing references for the node.
10. [NTP-C141 Create Optical Protection Groups for the ONS 15310-CL, page 4-12](#)—As needed, complete this procedure to set up optical protection groups for ONS 15310-CL ports.

11. [NTP-C142 Create Protection Groups for the ONS 15310-MA, page 4-13](#)—As needed, complete this procedure to set up protection groups for the ONS 15310-MA.
12. [NTP-C25 Set Up SNMP, page 4-15](#)—Complete this procedure if simple network management protocol (SNMP) will be used for network monitoring.
13. [NTP-C131 Provision OSI, page 4-16](#)—Complete this procedure if the ONS 15310-CL or ONS 15310-MA 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.

## NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL

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

- 
- Step 1** If you installed an Ethernet card, verify that it displays a solid green ACT (active) LED on the card faceplate.
- Step 2** To install a small-form factor pluggable (SFP) connector for the ONS 15310-CL, complete the [“DLP-C16 Install SFP Connectors” task on page 17-22](#). To remove an SFP, complete the [“DLP-C17 Remove SFP Connectors” task on page 17-23](#).
- Step 3** 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-C8 Install Optical Cables” procedure on page 1-12](#) for the ONS 15310-CL.
- Step 4** Verify that fiber is routed correctly in the shelf assembly.
- Step 5** Continue with the [“NTP-C20 Set Up Name, Date, Time, and Contact Information” procedure on page 4-4](#).
- Stop. You have completed this procedure.**
-

# NTP-C148 Verify Card and SFP Installation for the ONS 15310-MA

<b>Purpose</b>	This procedure verifies that the ONS 15310-MA node is ready for turn up.
<b>Tools/Equipment</b>	An engineering work order, site plan, or other document specifying the ONS 15310-MA card installation
<b>Prerequisite Procedures</b>	<a href="#">Chapter 2, “Install the Cisco ONS 15310-MA”</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** According to your site plan, verify that the CTX2500s are installed.
- Step 2** Verify that the green ACT (active) LED is illuminated on one CTX2500 and the amber STBY (standby) LED is illuminated on the second CTX2500.



**Note** If the CTX2500 cards are not installed, or if their LEDs are not illuminated as described, do not proceed. Repeat the [“NTP-C153 Install the CTX2500 Cards” procedure on page 2-16](#), or refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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-C155 Install the Electrical Cards” procedure on page 2-20](#).
- Step 4** If you installed an electrical card, verify that the electrical cables are installed. As necessary, complete the [“NTP-C158 Install the Electrical Cables” procedure on page 2-24](#).
- 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-C154 Install the Ethernet Cards” procedure on page 2-19](#).
- Step 6** To install a small-form factor pluggable (SFP) connector for the ONS 15310-MA, complete the [“DLP-C16 Install SFP Connectors” task on page 17-22](#). To remove an SFP, complete the [“DLP-C17 Remove SFP Connectors” task on page 17-23](#).
- 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-C160 Install Optical Cables” procedure on page 2-28](#) for the ONS 15310-MA.
- Step 8** Verify that fiber is routed correctly in the shelf assembly.
- Step 9** Continue with the [“NTP-C20 Set Up Name, Date, Time, and Contact Information” procedure on page 4-4](#).

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

---

## NTP-C19 Create Users and Assign Security

<b>Purpose</b>	This procedure creates ONS 15310-CL or ONS 15310-MA users and assigns their security levels.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser

- Step 1** Complete the “[DLP-C29 Log into CTC](#)” task on page 17-44 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-CL or ONS 15310-MA 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-C37 Create a New User on a Single Node](#)” task on page 17-51 or the “[DLP-C38 Create a New User on Multiple Nodes](#)” task on page 17-52 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-C83 Modify Users and Change Security](#)” procedure on page 11-6.

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

## NTP-C20 Set Up Name, Date, Time, and Contact Information

<b>Purpose</b>	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.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- Step 1** Complete the “[DLP-C29 Log into CTC](#)” task on page 17-44 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-CL and ONS 15310-MA users, complete the [“NTP-C35 Create a Logical Network Map” procedure on page 5-26](#). 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-CL or ONS 15310-MA 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-C75 Display Alarms and Conditions Using Time Zone” task on page 17-93](#).



**Note**

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

If you check the gateway network element (GNE) for the ONS 15310-CL or ONS 15310-MA 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-CL and Cisco ONS 15310-MA Reference Manual*.



**Caution**

If you reference another ONS 15310-CL or ONS 15310-MA 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-CL and ONS 15310-MA 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-CL and ONS 15310-MA clock is not running on battery backup, if power is lost the date and time must be reset.

- **Insert AIS-V on STS-1 SD-P**—Check this check box if you want AIS-Vs inserted on VT circuits carried by STS-1s when the STS-1 crosses its SD-P BER threshold. On protected circuits, traffic will be switched. If the switch cannot be performed, or if circuits are not protected, traffic will be dropped when the STS-1 SD-P BER threshold is reached.
- **SD-P BER**—If you selected Insert AIS-V, you can choose the SD-P BER level from the SD-P BER drop-down 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-C21 Set Up CTC Network Access” procedure on page 4-6](#).

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

## NTP-C21 Set Up CTC Network Access

<b>Purpose</b>	This procedure provisions network access for a node, including its subnet mask, default router, Dynamic Host Configuration Protocol (DHCP) server, IOP (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.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser

- 
- Step 1** Complete the “[DLP-C29 Log into CTC](#)” task on page 17-44. If you are already logged in, continue with Step 2.
- Step 2** Complete the “[DLP-C39 Provision IP Settings](#)” task on page 17-53 to provision the ONS 15310-CL or ONS 15310-MA IP address, subnet mask, default router, DHCP server, IOP listener port, and proxy server settings.
- Step 3** If you want to turn on the ONS 15310-MA secure mode, which allows two IPv4 addresses to be provisioned for the node if CTX2500 cards are installed, complete the “[DLP-C289 Enable Node Secure Mode](#)” task on page 19-93.
- Step 4** If static routes are needed, complete the “[DLP-C40 Create a Static Route](#)” task on page 17-55. Refer to the “Management Network Connectivity” chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for further information about static routes.
- Step 5** If the ONS 15310-CL or ONS 15310-MA 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-C41 Set Up or Change Open Shortest Path First Protocol](#)” task on page 17-56.
- Step 6** If the ONS 15310-CL or ONS 15310-MA is connected to a LAN or WAN that uses RIP, complete the “[DLP-C42 Set Up or Change Routing Information Protocol](#)” task on page 17-58.
- Step 7** Complete the “[DLP-C274 Provision the Designated SOCKS Servers](#)” task on page 19-89 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-C177 Set Up the ONS 15310 in EMS Secure Access

<b>Purpose</b>	This procedure provisions ONS 15310s and CTC computers for secure access.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-C21 Set Up CTC Network Access, page 4-6</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	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-C22 Set Up the ONS 15310-CL or ONS 15310-MA for Firewall Access

<b>Purpose</b>	This procedure provisions ONS 15310-CL nodes, ONS 15310-MA 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 and/or CTC computer, depending on whether one or both devices reside behind a firewall.
<b>Tools/Equipment</b>	IIOP listener port number provided by your LAN or firewall administrator
<b>Prerequisite Procedures</b>	<a href="#">NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL</a> , page 4-2
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

**Step 1** Complete the “[DLP-C29 Log into CTC](#)” task on page 17-44 at a node that is behind the firewall. If you are already logged in, continue with Step 2.

**Step 2** If the ONS 15310-CL or ONS 15310-MA node resides behind a firewall, complete the “[DLP-C43 Provision the IIOP Listener Port on the ONS 15310-CL or ONS 15310-MA](#)” task on page 17-59.

Figure 4-1 shows an ONS 15310-CL in a protected network and the CTC computer in an external network. For the computer to access the ONS 15310-CL/ONS 15310-MA nodes, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15310-CL/ONS 15310-MA.

**Figure 4-1** ONS 15310-CL Nodes Residing Behind a Firewall

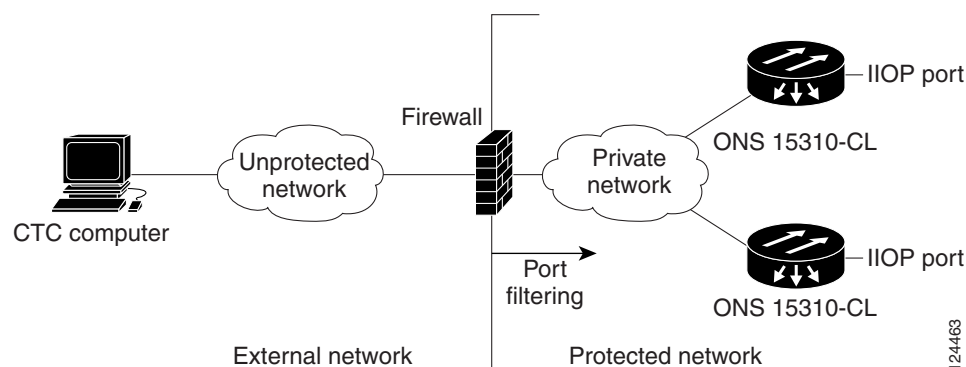
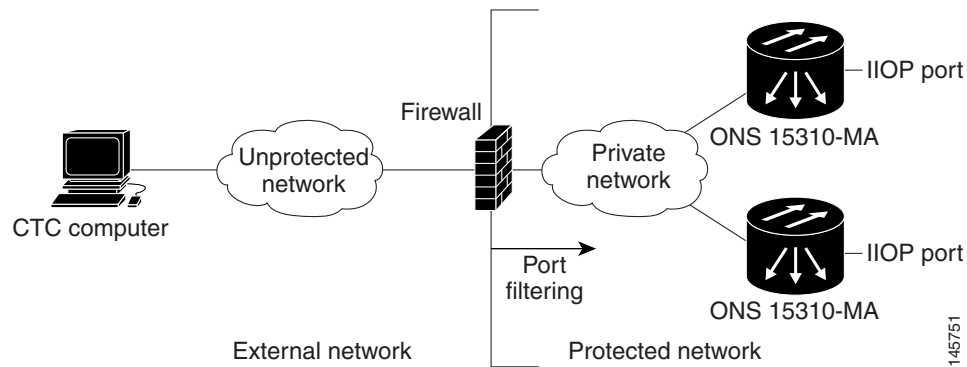




Figure 4-2 shows an ONS 15310-MA in a protected network and the CTC computer in an external network. For the computer to access the ONS 15310-CL/ONS 15310-MA nodes, you must provision the IIOp listener port specified by your firewall administrator on the ONS 15310-CL/ONS 15310-MA.

**Figure 4-2** ONS 15310-MA Nodes Residing Behind a Firewall



**Step 3** If the CTC computer resides behind a firewall, complete the “[DLP-C44 Provision the IIOp Listener Port on the CTC Computer](#)” task on page 17-60.

Figure 4-3 shows a CTC computer and ONS 15310-CL behind firewalls. For the computer to access the ONS 15310-CL, you must provision the IIOp port on the CTC computer and on the ONS 15310-CL.

**Figure 4-3** CTC Computer and ONS 15310-CLs Residing Behind Firewalls

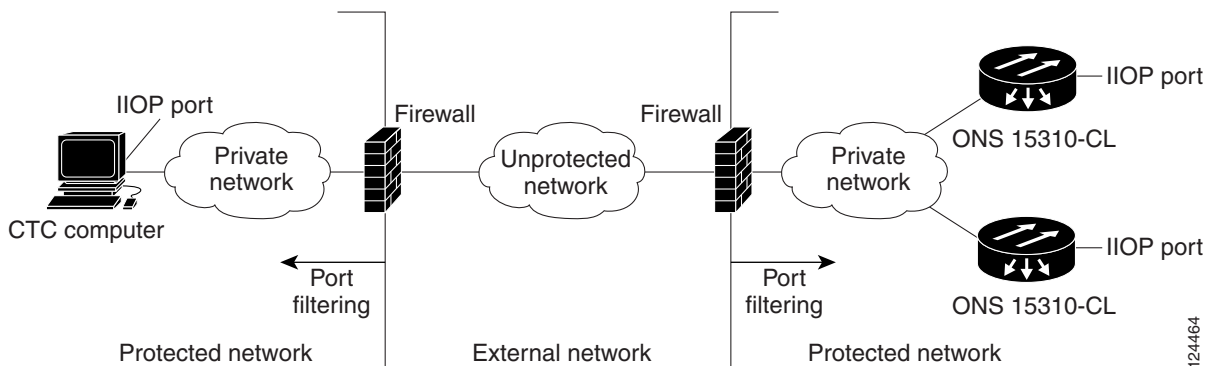
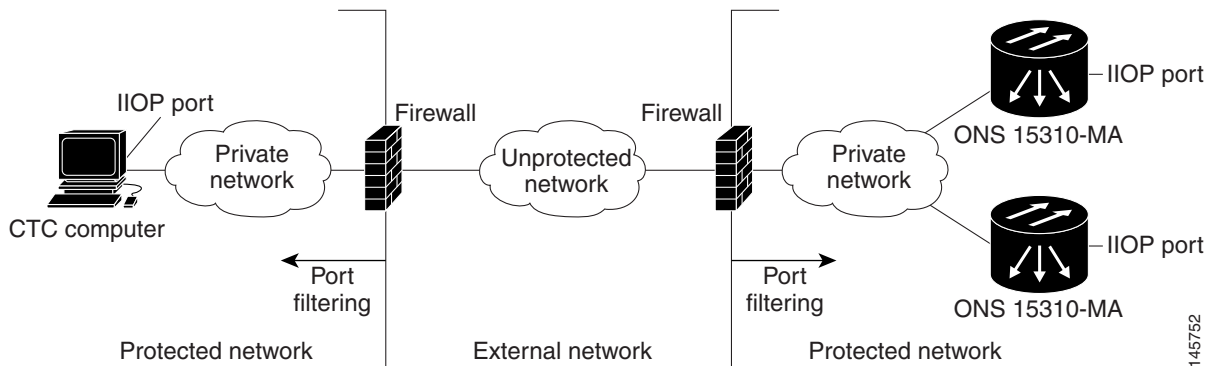


Figure 4-4 shows a CTC computer and ONS 15310-MA behind firewalls. For the computer to access the ONS 15310-MA, you must provision the IIOp port on the CTC computer and on the ONS 15310-MA.

Figure 4-4 CTC Computer and ONS 15310-MAs Residing Behind Firewalls



Step. You have completed this procedure.

## NTP-C276 Create FTP Host

<b>Purpose</b>	This procedure provisions FTP Host for access to ENEs for database backup. Use this procedure for database backup with FTP if proxy/firewall is enabled.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-C21 Set Up CTC Network Access, page 4-6</a> <a href="#">NTP-C22 Set Up the ONS 15310-CL or ONS 15310-MA for Firewall Access, page 4-8</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser

- 
- Step 1** Complete the “[DLP-C29 Log into CTC](#)” task on page 17-44 at the ONS 15310-CL or ONS 15310-MA node where you want to set up timing. If you are already logged in, continue with [Step 3](#).
- Step 2** If you want to turn on the ONS 15310-MA secure mode, which allows two IPv4 addresses to be provisioned for the node if CTX2500 cards are installed, complete the “[DLP-C289 Enable Node Secure Mode](#)” task on page 19-93.
- 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.
- Step 6** 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 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, skip to [Step 9](#)

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

## NTP-C23 Set Up Timing

<b>Purpose</b>	This procedure provisions the ONS 15310-CL or ONS 15310-MA timing.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** Complete the “[DLP-C29 Log into CTC](#)” task on page 17-44 at the ONS 15310-CL or ONS 15310-MA node where you want to set up timing. If you are already logged in, continue with Step 2.
- Step 2** Complete the “[DLP-C45 Set Up External or Line Timing](#)” task on page 17-61 if an external building integrated timing supply (BITS) source is available. This is the most common SONET timing setup procedure.
- Step 3** Complete the “[DLP-C46 Set Up Internal Timing](#)” task on page 17-63 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 SONET timing, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* or to Telcordia GR-253-CORE.

---

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

---

# NTP-C141 Create Optical Protection Groups for the ONS 15310-CL

<b>Purpose</b>	This procedure creates protection groups for ONS 15310-CL optical ports.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-C130 Manage Pluggable Port Modules, page 10-3</a> (optional) <a href="#">NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** Complete the [“DLP-C29 Log into CTC” task on page 17-44](#) 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 pluggable port modules (PPM) are provisioned for the same port and port rate on the 15310-CL-CTX where you will create the optical protection group.




---

**Note** PPMs are referred to as small-form factor pluggables (SFPs) in the hardware chapters.

---

You can use either of the following methods:

- In node view, move your mouse over the 15310-CL-CTX client port. If a PPM is provisioned, two dots appear in the port graphic, and the port and PPM port and rate appear when you move the mouse over the port.
- Display the 15310-CL-CTX in card view. Click the **Provisioning > Pluggable Port Module** tabs. Verify that a PPM is provisioned in the Pluggable Port Module area, and the port type and rate is provisioned for it in the Selected PPM area.

The PPM port and port rate must be the same for both 15310-CTX-CL ports. As necessary, complete the [“NTP-C130 Manage Pluggable Port Modules” procedure on page 10-3](#) to make PPM changes.

- Step 3** From node view, click the **Provisioning > Protection** tabs.
- Step 4** In the Protection Groups area, click **Create**.
- Step 5** In the Create Protection Group dialog box, enter the following:
- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (“) characters.
  - Type—Choose **1+1** from the drop-down list.
  - Protect Port—Choose the protect port from the drop-down list. The menu displays the available optical ports on the 15310-CL-CTX.
  - After you choose the protect port, a list of ports available for protection is displayed under Available Ports.
- Step 6** From the Available Ports list, choose the port that will be protected by the port you selected in the Protect Port field. Click the top arrow button to move the port to the Working Ports list.
- Step 7** Complete the remaining fields:

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

**Step 8** Click OK.

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

---

## NTP-C142 Create Protection Groups for the ONS 15310-MA

<b>Purpose</b>	This procedure creates ONS 15310-MA card protection groups.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-C130 Manage Pluggable Port Modules, page 10-3</a> (optional) <a href="#">NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

**Step 1** Complete the “[DLP-C29 Log into CTC](#)” task on page 17-44 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

[Table 4-1](#) describes the protection types available on the ONS 15310-MA.

**Table 4-1 Protection Types**

Type	Cards	Description and Installation Requirements
1:1	DS1-28/DS3-EC1-3 DS1-84/DS3-EC1-3	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 (MEA) state, because the 15310-MA 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 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 <i>Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual</i> .
1+1	CTX2500	Pairs a working OC-N port with a protect OC-N port. 1+1 protection can be created between any of the four total optical ports in any combination. For example, 1+1 can be created between two ports on the same CTX 2500 card, or it can be created between port 2-1 on one CTX2500 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.
Optimized 1+1	CTX2500	Ports must be provisioned to SDH. Optimized 1+1 protection is mainly used in networks that have linear 1+1 bidirectional protection schemes. Optimized 1+1 is a line-level protection scheme that includes two lines, working and protect. One of the two lines assumes the role of the primary channel, from which traffic gets selected, and the other port assumes the role of the secondary channel, which protects the primary channel. Traffic switches from the primary to the secondary channel based on either an external switching command or line conditions. After the line condition or the external switching command that was responsible for a switch clears, the roles of the two sides are reversed.
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.

**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-C242 Create a 1+1 Protection Group for the ONS 15310-MA, page 19-53](#)
- [DLP-C243 Create an Optimized 1+1 Protection Group for the ONS 15310-MA, page 19-55](#)



**Note** If a protect card is not installed, you can complete the “[NTP-C162 Preprovision a Card Slot](#)” procedure on page 2-31 and continue with the card protection provisioning.

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

## NTP-C25 Set Up SNMP

<b>Purpose</b>	This procedure provisions the SNMP parameters so that you can use SNMP management software with the ONS 15310-CL or ONS 15310-MA.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- Step 1** Complete the “[DLP-C29 Log into CTC](#)” task on page 17-44 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-CL or ONS 15310-MA network element (ENE), set the destination address to the GNE.
  - Community—Type the SNMP community name. For a description of SNMP community names, refer to the “SNMP” chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.



**Note** The community name is a form of authentication and access control. The community name assigned to the ONS 15310-CL or ONS 15310-MA 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-C225 Set Up SNMP for a GNE](#)” task on page 19-23 and “[DLP-C226 Set Up SNMP for an ENE](#)” task on page 19-24.

- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMP v1 or v2.
  - Max Traps Per Second—Choose a number from 0 to 32767. This field limits the number of traps per second to reduce network congestion.
- 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 gateway node elements (GNEs) and end node elements (ENEs), complete the following tasks as required, depending on the protection groups you want to create:
- [DLP-C225 Set Up SNMP for a GNE, page 19-23](#)
  - [DLP-C226 Set Up SNMP for an ENE, page 19-24](#)
  - [DLP-C227 Format and Enter NMS Community String for SNMP Command or Operation, page 19-26](#)
- Step 8** Click **Apply**.
- Stop. You have completed this procedure.**
- 

## NTP-C131 Provision OSI

<b>Purpose</b>	This procedure provisions the ONS 15310-CL or ONS 15310-MA 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.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	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-CL and Cisco ONS 15310-MA Reference Manual*.

---



### Caution

Do not begin this procedure until you know the role of the ONS 15310-CL or ONS 15310-MA 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-C29 Log into CTC](#)” task on page 17-44 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-C200 Provision OSI Routing Mode, page 19-1](#)—Complete this task first.
- [DLP-C201 Provision or Modify TARP Operating Parameters, page 19-2](#)—Complete this task next.
- [DLP-C202 Add a Static TID to NSAP Entry to the TARP Data Cache, page 19-4](#)—Complete this task as needed.
- [DLP-C204 Add a TARP Manual Adjacency Table Entry, page 19-5](#)—Complete this task as needed.
- [DLP-C205 Provision OSI Routers, page 19-6](#)—Complete this task as needed.
- [DLP-C206 Provision Additional Manual Area Addresses, page 19-6](#)—Complete this task as needed.
- [DLP-C207 Enable the OSI Subnet on the LAN Interface, page 19-7](#)—Complete this task as needed.
- [DLP-C208 Create an IP-Over-CLNS Tunnel, page 19-8](#)—Complete this task as needed.

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

---

