CHAPTER 19

DLPs C200 to C299

DLP-C200 Provision OSI Routing Mode

Purpose	This task provisions the Open System Interconnection (OSI) routing mode. Complete this task when the ONS 15310-CL or ONS 15310-MA is connected to networks with third party network elements (NEs) that use the OSI protocol stack for data communications network (DCN) communication.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Do not complete this task until you confirm the role of the node within the network. It will be either an ES or IS Level 1. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Caution Link State Protocol (LSP) buffers must be the same at all NEs within the network, or loss of visibility might occur. Do not modify the LSP buffers unless you confirm that all NEs within the OSI have the same buffer size.

Caution LSP buffer sizes cannot be greater than the LAP-D maximum transmission unit (MTU) size within the OSI area.

Note The ONS 15310 primary NSAP address is also the Router 1 primary manual area address. To edit the primary NSAP, you must edit the Router 1 primary manual area address. After you enable Router 1 on the Routers subtab, the Change Primary Area Address button is available to edit the address.

Step 1 In node view, click the **Provisioning** > **OSI** > **Main Setup** tabs.

Step 2 Choose a routing mode:

- End System—The ONS 15310 performs OSI end system (ES) functions and relies upon an intermediate system (IS) for communication with nodes that reside within its OSI area.

  Note The End System routing mode is not available if more than one virtual router is enabled.

- Intermediate System Level 1—The ONS 15310 performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.

Step 3 If needed, change the L1 LSP Buffer Size. This adjusts the Level 1 link state protocol data unit (PDU) buffer size. The default is 512. It should not be changed.

Step 4 Return to your originating procedure (NTP).

DLP-C201 Provision or Modify TARP Operating Parameters

Purpose	This task provisions or modifies the Target Identifier Address Resolution Protocol (TARP) operating parameters including TARP PDU propagation, timers, and loop detection buffer (LDB).
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > OSI > TARP > Config** tabs.

Step 2 Provision the following parameters, as needed:

- TARP PDUs L1 Propagation—If checked (default), TARP Type 1 PDUs that are received by the node and are not excluded by the LDB are propagated to other NEs within the Level 1 OSI area. (Type 1 PDUs request a protocol address that matches a target identifier [TID] within a Level 1 routing area.) The propagation does not occur if the NE is the target of the Type 1 PDU, and PDUs are not propagated to the NE from which the PDU was received.

  Note This parameter is not used when the Node Routing Area (Provisioning > OSI > Main Setup tab) is set to End System.

- TARP PDUs Origination—If checked (default), the node performs all TARP origination functions including:
  - TID to Network Service Access Point (NSAP) resolution requests (originate TARP Type 1 and Type 2 PDUs)
  - NSAP to TID requests (originate Type 5 PDUs)
  - TARP address changes (originate Type 4 PDUs)

Note TARP Echo is not supported.

- TARP Data Cache—If checked (default), the node maintains a TARP data cache (TDC). The TDC is a database of TID to NSAP pairs created from TARP Type 3 PDUs received by the node and modified by TARP Type 4 PDUs (TID to NSAP updates or corrections). TARP 3 PDUs are responses to Type 1 and Type 2 PDUs. The TDC can also be populated with static entries entered on the TARP > Static TDC tab.

Note This parameter is only used when the TARP PDUs Origination parameter is enabled.

- LDB—If checked (default), enables the TARP loop detection buffer. The LDB prevents TARP PDUs from being sent more than once on the same subnet.

Note The LDP parameter is not used if the Node Routing Mode is provisioned to End System or if the TARP PDUs L1 Propagation parameter is not enabled.

- LAN TARP Storm Suppression—If checked (default), enables TARP storm suppression. This function prevents redundant TARP PDUs from being unnecessarily propagated across the LAN network.
- Send Type 4 PDU on Startup—If checked, a TARP Type 4 PDU is originated during the initial ONS 15310 startup. Type 4 PDUs indicate that a TID or NSAP change has occurred at the NE. (The default setting is not enabled.)
- Type 4 PDU Delay—Sets the amount of time that will pass before the Type 4 PDU is generated when Send Type 4 PDU on Startup is enabled. 60 seconds is the default. The range is 0 to 255 seconds.

Note The Send Type 4 PDU on Startup and Type 4 PDU Delay parameters are not used if TARP PDUs Origination is not enabled.

- LDB Entry—Sets the TARP loop detection buffer timer. The LDB buffer time is assigned to each LDB entry for which the TARP sequence number (tar-seq) is zero. The default is 5 minutes. The range is 1 to 10 minutes.
- LDB Flush—Sets the frequency period for flushing the LDB. The default is 5 minutes. The range is 0 to 1440 minutes.
- T1—Sets the amount of time to wait for a response to a Type 1 PDU. Type 1 PDUs seek a specific NE TID within an OSI Level 1 area. The default is 15 seconds. The range is 0 to 3600 seconds.
- T2—Sets the amount of time to wait for a response to a Type 2 PDU. TARP Type 2 PDUs seek a specific NE TID value within OSI Level 1 and Level 2 areas. The default is 25 seconds. The range is 0 to 3600 seconds.
- T3—Sets the amount of time to wait for an address resolution request. The default is 40 seconds. The range is 0 to 3600 seconds.
- T4—Sets the amount of time to wait for an error recovery. This timer begins after the T2 timer expires without finding the requested NE TID. The default is 20 seconds. The range is 0 to 3600 seconds.

Note Timers T1, T2, and T4 are not used if TARP PDUs Origination is not enabled.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-C202 Add a Static TID to NSAP Entry to the TARP Data Cache

Purpose	This task adds a static TID to NSAP entry to the TDC. The static entries are required for NEs that do not support TARP and are similar to static routes. For a specific TID, you must force a specific NSAP.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

Step 1 In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.

Step 2 Click **Add Static Entry**.

Step 3 In the Add Static Entry dialog box, enter the following:

- TID—Enter the TID of the NE. (For ONS nodes, the TID is the Node Name parameter on the node view Provisioning > General tab.)
- NSAP—Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.

Step 4 Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-C203 Remove a Static TID to NSAP Entry from the TARP Data Cache

Purpose	This task removes a static TID to NSAP entry from the Tarp Data Cache (TDC).
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

Step 1 In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.

Step 2 Click the static entry that you want to delete.

Step 3 Click **Delete Static Entry**.

Step 4 In the Delete TDC Entry dialog box, click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-C204 Add a TARP Manual Adjacency Table Entry

Purpose	This task adds an entry to the TARP manual adjacency table (MAT). Entries are added to the MAT when the ONS 15310-CL or ONS 15310-MA must communicate across routers or non-SONET NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Provisioning > OSI > TARP > MAT** tabs.

Step 2 Click **Add**.

Step 3 In the Add TARP Manual Adjacency Table Entry dialog box, enter the following:

- Level—Sets the TARP Type Code that will be sent:
  - **Level 1**—Indicates that the adjacency is within the same area as the current node. The entry generates Type 1 PDUs.
  - **Level 2**—Indicates that the adjacency is in a different area than the current node. The entry generates Type 2 PDUs.
- NSAP—Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.

Step 4 Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-C205 Provision OSI Routers

Purpose	This task enables the OSI virtual router and edits its primary manual area address.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The Router 1 manual area address, System ID, and Selector "00" create the node NSAP address. Changing the Router 1 manual area address changes the node's NSAP address.

Note The System ID for Router 1 is the node MAC address.

Step 1 In node view, click the **Provisioning > OSI > Routers > Setup** tabs.

Step 2 Chose the router you want provision and click **Edit**.

Step 3 In the OSI Router Editor dialog box:

a. Check **Enable Router** to enable the router and make its primary area address available for editing.

b. Click the manual area address, then click **Edit**.

c. In the Edit Manual Area Address dialog box, edit the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the edits in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 8 to 24 alphanumeric characters (0–9, a–f) in length.

d. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Edit Manual Area Address, and OSI Router Editor.

Step 4 Return to your originating procedure (NTP).

DLP-C206 Provision Additional Manual Area Addresses

Purpose	This task provisions the OSI manual area addresses. Three additional manual areas can be created for each virtual router.
Tools/Equipment	None
Prerequisite Procedures	DLP-C205 Provision OSI Routers, page 19-6 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Provisioning > OSI > Routers > Setup** tabs.

Step 2 Chose the router where you want provision an additional manual area address and click **Edit**. The OSI Router Editor dialog box appears.

Step 3 In the OSI Router Editor dialog box:

a. Check **Enable Router** to enable the router and make its primary area address available for editing.

b. Click the manual area address, then click **Add**.

c. In the Add Manual Area Address dialog box, enter the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 2 to 24 alphanumeric characters (0–9, a–f) in length.

d. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Add Manual Area Address, and OSI Router Editor.

Step 4 Return to your originating procedure (NTP).

DLP-C207 Enable the OSI Subnet on the LAN Interface

Purpose	This task enables the OSI subnetwork point of attachment on the LAN interface.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note OSI subnetwork points of attachment are enabled on DCCs when you create DCCs. See the "DLP-C52 Provision Section DCC Terminations" task on page 17-68 and the "DLP-C53 Provision Line DCC Terminations" task on page 17-70.

Note The OSI subnetwork point of attachment cannot be enabled for the LAN interface if the OSI routing mode is set to ES (end system).

Note If Secure Mode is on, the OSI Subnet is enabled on the backplane LAN port, not the front TCC2P port.

Step 1 In node view, click the **Provisioning > OSI > Routers > Subnet** tabs.

Step 2 Click **Enable LAN Subnet**.

Step 3 In the Enable LAN Subnet dialog box, complete the following fields:

- ESH—Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.

- ISH—Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
- IS-IS Cost—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default IS-IS cost for LAN subnets is 20. It normally should not be changed.
- DIS Priority—Sets the designated intermediate system (DIS) priority. In IS-IS networks, one router is elected to serve as the DIS (LAN subnets only). Cisco router DIS priority is 64. For the ONS 15310-CL or ONS 15310-MA LAN subnet, the default DIS priority is 63. It normally should not be changed.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C208 Create an IP-Over-CLNS Tunnel

Purpose	This task creates an IP-over-CLNS tunnel to allow ONS 15310-CL or ONS 15310-MA nodes to communicate across equipment and networks that use the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution IP-over-CLNS tunnels require two end points. You will create one point on an ONS 15310-CL or ONS 15310-MA. The other end point is generally provisioned on non-ONS equipment including routers and other vendor NEs. Before you begin, verify that you have the capability to create an IP-over-CLNS tunnel on the other equipment location.

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

Step 2 Click **Create**.

Step 3 In the Create IP Over CLNS Tunnel dialog box, complete the following fields:

- Tunnel Type—Choose a tunnel type:
  - Cisco—Creates the proprietary Cisco IP tunnel. Cisco IP tunnels add the CLNS header to the IP packets.
  - GRE—Creates a Generic Routing Encapsulation tunnel. GRE tunnels add the CLNS header and a GRE header to the IP packets.

The Cisco proprietary tunnel is slightly more efficient than the GRE tunnel because it does not add the GRE header to each IP packet. The two tunnel types are not compatible. Most Cisco routers support the Cisco IP tunnel, while only a few support both GRE and Cisco IP tunnels. You generally should create Cisco IP tunnels if you are tunneling between two Cisco routers or between a Cisco router and an ONS node.

Caution Always verify that the IP-over-CLNS tunnel type you choose is supported by the equipment at the other end of the tunnel.

- Node Address—Enter the IP address of the IP-over-CLNS tunnel destination.
- Subnet Mask—Enter the IP address subnet mask of the IP-over-CLNS destination.
- OSPF Cost—Enter the Open Shortest Path First (OSPF) metric for sending packets across the IP-over-CLNS tunnel. The OSPF metric, or cost, is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not be changed unless you are creating multiple tunnel routes and want to prioritize routing by assigning different metrics.
- NSAP Address—Enter the destination NE or OSI router NSAP address.

Step 4 Click **OK**.

Step 5 Provision the other tunnel end point.

Step 6 Return to your originating procedure (NTP).

DLP-C209 Remove a TARP Manual Adjacency Table Entry

Purpose	This task removes an entry from the TARP manual adjacency table.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If TARP manual adjacency is the only means of communication to a group of nodes, loss of visibility will occur when the adjacency table entry is removed.

Step 1 In node view, click the **Provisioning > OSI > TARP > MAT** tabs.

Step 2 Click the MAT entry that you want to delete.

Step 3 Click **Remove**.

Step 4 In the Delete TDC Entry dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C211 Edit the OSI Router Configuration

Purpose	This task edits the OSI router configuration, including enabling and disabling OSI routers, editing the primary area address, and creating or editing additional area addresses.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > OSI > Routers > Setup** tabs.

Step 2 Choose the router you want provision and click **Edit**.

Step 3 In the OSI Router Editor dialog box:

a. Check or uncheck the Enabled box to enable or disable the router.

Note Router 1 must be enabled before you can enable Routers 2 and 3.

b. For enabled routers, edit the primary area address, if needed. The address can be between 8 and 24 alphanumeric characters in length.

c. If you want to add or edit an area address to the primary area, enter the address at the bottom of the Multiple Area Addresses area. The area address can be 2 to 26 numeric characters (0–9) in length. Click **Add**.

d. Click **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-C212 Edit the OSI Subnetwork Point of Attachment

Purpose	This task allows you to view and edit the OSI subnetwork point of attachment parameters. The parameters are initially provisioned when you create a Section DCC (SDCC), Line DCC (LDCC), generic communications channel (GCC), or optical service channel (OSC), or when you enable the LAN subnet.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Provisioning > OSI > Routers > Subnet** tabs.

Step 2 Choose the subnet you want to edit, then click **Edit**.

Step 3 In the Edit <*subnet type*> Subnet <*slot/port*> dialog box, edit the following fields:

- ESH—The End System Hello PDU propagation frequency. An end system NE transmits ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—The Intermediate System Hello PDU propagation frequency. An intermediate system NE sends ISHs to other ESs and ISs to inform them about the NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—The Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.

Note The IS-IS Cost and DIS Priority parameters are provisioned when you create or enable a subnet. You cannot change the parameters after the subnet is created. To change the DIS Priority and IS-IS Cost parameters, delete the subnet and create a new one.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C213 Edit an IP-Over-CLNS Tunnel

Purpose	This task edits the parameters of an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-C208 Create an IP-Over-CLNS Tunnel, page 19-8 DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Changing the IP or NSAP addresses or an IP-over-CLNS tunnel can cause loss of NE visibility or NE isolation. Do not change network addresses until you verify the changes with your network administrator.

Step 1 Click the **Provisioning > OSI > Tunnels** tabs.

Step 2 Click **Edit**.

Step 3 In the Edit IP Over OSI Tunnel dialog box, complete the following fields:

- Tunnel Type—Edit the tunnel type:
  - **Cisco**—Creates the proprietary Cisco IP tunnel. Cisco IP tunnels add the CLNS header to the IP packets.
  - **GRE**—Creates a Generic Routing Encapsulation tunnel. GRE tunnels add the CLNS header and a GRE header to the IP packets.

The Cisco proprietary tunnel is slightly more efficient than the GRE tunnel because it does not add the GRE header to each IP packet. The two tunnel types are not compatible. Most Cisco routers support the Cisco IP tunnel, while only a few support both GRE and Cisco IP tunnels. You generally should create Cisco IP tunnels if you are tunneling between two Cisco routers or between a Cisco router and an ONS node.

Caution Always verify that the IP-over-CLNS tunnel type you choose is supported by the equipment at the other end of the tunnel.

- IP Address—Enter the IP address of the IP-over-CLNS tunnel destination.
- IP Mask—Enter the IP address subnet mask of the IP-over-CLNS destination.
- OSPF Metric—Enter the OSPF metric for sending packets across the IP-over-CLNS tunnel. The OSPF metric, or cost, is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not be changed unless you are creating multiple tunnel routes and want to prioritize routing by assigning different metrics.
- NSAP Address—Enter the destination NE or OSI router NSAP address.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C214 Delete an IP-Over-CLNS Tunnel

Purpose	This task allows you to delete an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting an IP-over-CLNS tunnel might cause the nodes to loose visibility or cause node isolation. If node isolation occurs, onsite provisioning might be required to regain connectivity. Always confirm tunnel deletions with your network administrator.

Step 1 Click the **Provisioning > OSI > Tunnels** tabs.

Step 2 Choose the IP-over-CLNS tunnel that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C215 View IS-IS Routing Information Base

Purpose	This task allows you to view the Intermediate System-to-Intermediate-System (IS-IS) protocol routing information base (RIB). IS-IS is an OSI routing protocol that floods the network with information about NEs on the network. Each NE uses the information to build a complete and consistent picture of a network topology. The IS-IS RIB shows the network view from the perspective of the IS node.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Maintenance** > **OSI** > **IS-IS RIB** tabs.

Step 2 View the following RIB information for Router 1:

- Subnet Type—Indicates the OSI subnetwork point of attachment type used to access the destination address. Subnet types include SDCC, LDCC, GCC, OSC, and LAN.
- Location—Indicates the OSI subnetwork point of attachment. For DCC subnets, the slot and port are displayed. LAN subnets are shown as LAN.
- Destination Address—The destination network service access point (NSAP) of the IS.
- MAC Address—For destination NEs that are accessed by LAN subnets, the NE's MAC address.

Step 3 If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.

Step 4 Return to your originating procedure (NTP).

DLP-C216 View ES-IS Routing Information Base

Purpose	This task allows you to view the End-System-to-Intermediate-System (ES-IS) protocol RIB. ES-IS is an OSI protocol that defines how end systems (hosts) and intermediate systems (routers) learn about each other. For ESs, the ES-IS RIB shows the network view from the perspective of the ES node. For ISs, the ES-IS RIB shows the network view from the perspective of the IS node.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Maintenance** > **OSI** > **ES-IS RIB** tabs.

Step 2 View the following RIB information for Router 1:

- Subnet Type—Indicates the OSI subnetwork point of attachment type used to access the destination address. Subnet types include SDCC, LDCC, GCC, OSC, and LAN.
- Location—Indicates the subnet interface. For DCC subnets, the slot and port are displayed. LAN subnets are shown as LAN.
- Destination Address—The destination IS NSAP.
- MAC Address—For destination NEs that are accessed by LAN subnets, the NE's MAC address.

Step 3 If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.

Step 4 Return to your originating procedure (NTP).

DLP-C217 Manage the TARP Data Cache

Purpose	This task allows you to view and manage the TARP data cache (TDC). The TDC facilitates TARP processing by storing a list of TID-to-NSAP mappings.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Maintenance** > **OSI** > **TDC** tabs.

Step 2 View the following TARP data cache information:

- TID—The target identifier of the originating NE. For ONS 15454s, the TID is the name entered in the Node Name/TID field on the Provisioning > General tab.
- NSAP/NET—The NSAP or Network Element Title (NET) of the originating NE.
- Type—Indicates how the TDC entry was created:
  - Dynamic—The entry was created through the TARP propagation process.
  - Static—The entry was manually created and is a static entry.

Step 3 If you want to query the network for an NSAP that matches a TID, complete the following steps. Otherwise, continue with Step 4.

Note The TID to NSAP function is not available if the TDC is not enabled on the Provisioning > OSI > TARP tab.

a. Click the **TID to NSAP** button.

b. In the TID to NSAP dialog box, enter the TID that you want to map to an NSAP.

c. Click **OK**, then click **OK** in the information message.

d. On the TDC tab, click **Refresh**.

If TARP finds the TID in its TDC, it returns the matching NSAP. If not, TARP sends PDUs across the network. Replies will return to the TDC later, and a "check TDC later" message is displayed.

Step 4 If you want to delete all the dynamically generated TDC entries, click the **Flush Dynamic Entries** button. If not, continue with Step 5.

Step 5 Return to your originating procedure (NTP).

DLP-C218 Soft-Reset a 15310-CL-CTX or CTX2500 Card Using CTC

Purpose	This task resets a 15310-CL-CTX (ONS 15310-CL) or CTX2500 (ONS 15310-MA) card using a soft reset. A soft reset reboots the card and reloads the operating system and the application software. If there are two CTX2500 cards installed on the ONS 15310 MA the standby CTX2500 will become active after issuing an active CTX soft-reset.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Caution Soft-resetting the 15310-CL-CTX or CTX2500 cards causes a traffic hit only if a provisioning change or firmware update has occurred. Otherwise, the soft reset is errorless.

Caution Do not soft reset more than one ONS 15310-MA card at a time. Instead, issue a soft reset command for a single card, then wait until CTC shows the card is back up. You can then issue a soft reset on another card if needed. Completing soft resets in sequence helps to avoid unexpected traffic hits.

Note Before you reset the 15310-CL-CTX or CTX2500 card, you should wait at least 60 seconds after the last provisioning change to avoid losing any changes to the database.

Note The 15310-CL-CTX and CTX2500 cards do not support a real time clock with battery backup. Hence, during a card reset, the time is reset to default and the date starts at 1970 till you set the time/date again.

Note A software reset causes a standard Telcordia protection switch of less than 50 ms.

Step 1 In node view, right-click the 15310-CL-CTX card or the CTX2500 card to reveal a drop-down list.

Step 2 Click **Soft-Reset Card**.

Note For an ONS 15310-MA, if there is any condition that prevents an errorless soft-reset, the "Force Soft-Reset" message appears. You can choose to abort the soft-reset or proceed with the forced soft-reset.

Step 3 Click **Yes** when the "Are You Sure?" dialog box appears.

Step 4 Return to your originating procedure (NTP).

DLP-C219 Hard-Reset the 15310-CL-CTX or CTX2500 Card Using CTC

Purpose	This task resets the 15310-CL-CTX card (ONS 15310-CL) or CTX2500 card (ONS 15310-MA) using a hard reset. A hard reset temporarily removes power from the card and clears all buffer memory.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Caution Typically a hard reset causes a standard Telcordia protection switch of less than 50 ms. However, in the following scenarios, hard-resetting the 15310-CL-CTX or CTX2500 cards causes a traffic loss until the 15310-CL-CTX or CTX2500 card fully resets:

If a 1+1 protection group is provisioned between optical ports located on the same 15310-CL-CTX or CTX2500 card.

If both paths of a path protection configuration traverse through optical ports on the same 15310-CL-CTX or CTX2500.

Note Before you reset the 15310-CL-CTX or CTX2500 card, you should wait at least 60 seconds after the last provisioning change to avoid losing any changes to the database.

Note The 15310-CL-CTX and CTX2500 cards do not support a real time clock with battery backup. Hence, during a card reset, the time is reset to default and the date starts at 1970 till you set the time/date again.

Step 1 In node view, click the **Inventory** tab. Locate the 15310-CL-CTX or CTX2500 card in the inventory pane.

Step 2 Click the **Admin State** drop-down list and select **OOS-MT**. Click **Apply**.

Step 3 Click **Yes** in the "Action may be service affecting. Are you sure?" dialog box.

Step 4 The service state of the card becomes OOS-MA,MT. The card faceplate appears blue in CTC.

Step 5 Right-click the card to reveal a shortcut menu.

Step 6 Click **Hard-reset Card**.

Step 7 Click **Yes** in the “Are you sure you want to hard-reset this card?” dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-C220 Soft-Reset an Ethernet or Electrical Card Using CTC

Purpose	This task resets the ML-100T-8, CE-100T-8, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card using a soft reset. A soft reset reboots the card and reloads the operating system and the application software.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Caution Do not soft reset more than one ONS 15310-MA card at a time. Instead, issue a soft reset command for a single card, then wait until CTC shows the card is back up. You can then issue a soft reset on another card if needed. Completing soft resets in sequence helps to avoid unexpected traffic hits.

Caution Soft-resetting an Ethernet card causes a traffic hit. However, soft-resetting a traffic card is errorless in most cases. If there is a provisioning change during the soft reset, or if the firmware is replaced during the software upgrade process, the reset is not errorless.

Step 1 In node view, right-click the card to reveal a shortcut menu.

Step 2 Click **Soft-reset Card**.

Step 3 Click **Yes** in the “Are you sure you want to soft-reset this card?” dialog box.

Step 4 Return to your originating procedure (NTP).

DLP-C221 Hard-Reset an Ethernet or Electrical Card Using CTC

Purpose	This task resets the ML-100T-8, CE-100T-8, DS1-28/DS3-EC1-3, or DS1-28/DS3-EC1-3 card using a hard reset. A hard reset temporarily removes power from the card and clears all buffer memory before it is physically reseated.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Caution Hard-resetting a traffic card causes a traffic hit.

Note The hard-reset option is enabled only when the card is placed in the OOS-MA,MT service state.

Step 1 In node view, click the **Inventory** tab. Locate the appropriate card in the inventory pane.

Step 2 Click the **Admin State** drop-down list and select **OOS-MT**. Click **Apply**.

Step 3 Click **Yes** in the “Action may be service affecting. Are you sure?” dialog box.

Step 4 The service state of the card becomes OOS-MA,MT. The card faceplate appears blue in CTC and the SRV LED turns amber.

Step 5 Right-click the card to reveal a shortcut menu.

Step 6 Click **Hard-reset Card**.

Step 7 Click **Yes** in the “Are you sure you want to hard-reset this card?” dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-C222 Print CTC Data

Purpose	This task prints CTC card, node, or network data in graphical or tabular form on a Windows-provisioned printer.
Tools/Equipment	Printer connected to the CTC computer by a direct or network connection
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the CTC tab (and subtab, if present) containing the information you want to print. For example, click the **Alarms** tab to print Alarms window data.

The print operation is available for all network, node (default login), and card view windows.

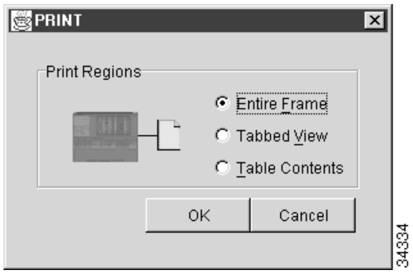
Step 2 From the File menu, choose **Print**.

Step 3 In the Print dialog box, click a a printing option (Figure 19-1).

- Entire Frame—Prints the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.
- Tabbed View—Prints the lower half of the CTC window containing tabs and data. The printout includes the selected tab (on top) and the data shown in the tab window. For example, if you print the History window Tabbed View, you print only history items appearing in the window. This option is available for all windows.
- Table Contents—Prints CTC data in table format without graphical representations of shelves, cards, or tabs.The Table Contents option prints all the data contained in a table with the same column headings. For example, if you print the History window Table Contents view, you print all data included in the table whether or not items appear in the window.

Tip When you print using the Tabbed View option, it can be difficult to determine whether the printout applies to the network, node, or card view. Look at the tabs to determine which view you are printing. Network, node, and card views are identical except that network view does not contain an Inventory tab; node view and card view contain a Performance tab.

Figure 19-1 Selecting CTC Data For Print



Step 4 Click **OK**.

Step 5 In the Windows Print dialog box, click a printer and click **OK.**

Step 6 Repeat this task for each window that you want to print.

Step 7 Return to your originating procedure (NTP).

DLP-C223 Export CTC Data

Purpose	This task exports CTC table data as delineated text to view or edit the data in text editor, word processing, spreadsheet, database management, or web browser applications. You can also export data from the Edit Circuits window.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the CTC tab containing the information you want to export (for example, the Alarms tab or the Circuits tab).

Step 2 If you want to export detailed circuit information, complete the following:

a. In the Circuits window, choose a circuit and click **Edit** to open it in the Edit Circuits window.

b. In the Edit Circuits window, choose the desired tab: **Drops**, **Path Protection Selectors**, **Path Protection Switch Counts**, **State**, or **Merge**.

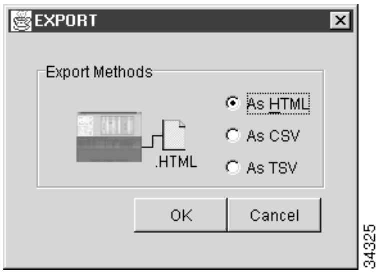
Note Depending upon your configuration, you might or might not see all of the listed tabs when you click Edit.

Step 3 From the File menu, choose **Export**.

Step 4 In the Export dialog box (Figure 19-2), click a data format:

- **As HTML**—Saves data as a simple HTML table file without graphics. The file must be viewed or edited with applications such as Netscape Navigator, Microsoft Internet Explorer, or other applications capable of opening HTML files.
- **As CSV**—Saves the CTC table as comma-separated values (CSV). This option does not apply to the Maintenance > Timing > Report tab.
- **As TSV**—Saves the CTC table as tab-separated values (TSV).

Figure 19-2 Selecting CTC Data For Export



Step 5 If you want to open a file in a text editor or word processor application, procedures vary. Typically you can use the File > Open command to display the CTC data, or you can double-click the file name and choose an application such as Notepad.

Text editor and word processor applications display the data exactly as it is exported, including comma or tab separators. All applications that open the data files allow you to format the data.

Step 6 If you want to open the file in spreadsheet and database management applications, procedures vary. Typically you need to open the application and choose File > Import, then choose a delimited file to display the data in cells.

Spreadsheet and database management programs also allow you to manage the exported data.

Note An exported file cannot be opened in CTC.

The export operation applies to all tabular data except the following:

- Circuits (Edit option, General, and Monitor tabs)
- Provisioning > General tab
- Provisioning > Network > General tab
- Provisioning > Orderwire tab
- Provisioning > Security > Policy, Data Comm, Access, and Legal Disclaimer tabs
- Provisioning > SNMP tab
- Provisioning > Timing > General and BITS Facilities tabs
- Provisioning > OSI > Main Setup tab
- Provisioning > OSI > TARP > Config tab
- Maintenance > Database tab
- Maintenance > Diagnostic tab
- Maintenance > Protection tab
- Maintenance > Timing > Source tab

Step 7 Click **OK**.

Step 8 In the Save dialog box, enter a name in the File name field using one of the following formats:

- *filename*.html for HTML files
- *filename*.csv for CSV files
- *filename*.tsv for TSV files

Step 9 Navigate to the directory where you want to store the file.

Step 10 Click **OK**.

Step 11 Repeat the task for each window that you want to export.

Step 12 Return to your originating procedure (NTP).

DLP-C224 Change Optics Thresholds Settings for Optical Ports

Purpose	This task changes the optics threshold settings on optical ports. Optical ports on the ONS 15310-CL and ONS 15310-MA are provided through Small Form-factor Pluggables (SFPs) installed on the 15310-CL-CTX card (ONS 15310-CL) and the CTX2500 card (ONS 15310-MA).
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the 15310-CL-CTX card or the CTX2500 card.

Step 2 Click the **Provisioning > Optical > Optics Thresholds** tabs.

Note If you want to modify a threshold setting, it might be necessary to click the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 3 Modify the settings described in Table 19-1 by clicking in the field that you want to modify. In some fields, you can choose an option from a drop-down list; in others you can type a value.

Note You must set the normalized optical power received (OPR) value whenever you replace or insert an SFP. After you click Set for the port you are observing, the LBC (%), OPR (%), and OPT (%) values under the Performance > Optical tabs should be close to 100 percent. Only Cisco-approved SFPs should be used. See Chapter 1, "Install the Cisco ONS 15310-CL" or Chapter 2, "Install the Cisco ONS 15310-MA" for more information about installing SFPs and fiber-optic cable.

Table 19-1 Optics Thresholds Settings

Parameter	Description	Options
Port	(Display only) Port number.	• 1-1 • 2-1
LBC-LOW	Laser bias current–minimum.	Default (15 min/1 day): 50 percent
LBC-HIGH	Laser bias current–maximum.	Default (15 min/1 day): 150 percent
OPT-LOW	Optical power transmitted–minimum.	Default (15 min/1 day): 80 percent
OPT-HIGH	Optical power transmitted–maximum.	Default (15 min/1 day): 120 percent
OPR-LOW	Optical power received–minimum.	Default (15 min/1 day): 50 percent
OPR-HIGH	Optical power received–maximum.	Default (15 min/1 day): 200 percent

Table 19-1 Optics Thresholds Settings (continued)

Parameter	Description	Options
Set OPR	Setting the optical power received establishes the received power level as 100 percent. If the receiver power decreases, then the OPR percentage decreases to reflect the loss in receiver power. For example, if the receiver power decreases by 3 dBm, the OPR decreases 50 percent.	Click **SET**.
Types	Sets the type of alert that occurs when a threshold is crossed. To change the type of threshold, choose one and click **Refresh**.	• TCA (threshold crossing alert) • Alarm
Intervals	Sets the time interval for collecting parameter counts. To change the time interval, choose the desired interval and click **Refresh**.	• 15 Min • 1 Day

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-C225 Set Up SNMP for a GNE

Purpose	This procedure provisions simple network management protocol (SNMP) parameters so that you can use SNMP network management software with the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Step 2 In the Trap Destinations area, click **Create**.

Step 3 On the Create SNMP Trap Destination dialog box, complete the following fields:

- Destination Node Address—Enter the IP address of your network management system (NMS).
- Community—Enter the SNMP community name. (For more information about SNMP, 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 is case-sensitive and must match the community name of the NMS.

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

Step 4 Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.

Step 5 Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.

Step 6 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 7 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the **Enable SNMP Proxy** check box on the SNMP tab.

Note The ONS firewall proxy feature only operates on nodes running releases 4.6 and later. Using this information effectively breaches the ONS firewall to exchange management information.

For more information about the SNMP proxy feature, refer to the “SNMP” chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 8 Click **Apply**.

Step 9 Return to your originating procedure (NTP).

DLP-C226 Set Up SNMP for an ENE

Purpose	This procedure provisions the SNMP parameters for an ONS 15310-CL or ONS 15310-MA configured to be an ENE if you use SNMP proxy on the GNE.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Step 2 In the Trap Destinations area, click **Create**.

Step 3 On the Create SNMP Trap Destination dialog box, complete the following fields:

- Destination Node Address—Enter the IP address of your NMS.

- Community—Enter the SNMP community name. (For more information about SNMP, 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 is case-sensitive and must match the community name of the NMS.

- UDP Port—The default UDP port for SNMP traps is 162.
- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

Step 4 Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.

Step 5 Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.

Step 6 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 7 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the **Enable SNMP Proxy** check box on the SNMP tab.

Note The ONS firewall proxy feature only operates on nodes running releases 4.6 and later. Using this information effectively breaches the ONS firewall to exchange management information.

For more information about the SNMP proxy feature, refer to the "SNMP" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 8 Click **Apply**.

Step 9 If you are setting up SNMP proxies, you can set up to three relays for each trap address to convey SNMP traps from the NE to the NMS. To do this, complete the following substeps:

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

b. If the node you are logged into is an ENE, set the Relay A address to the GNE and type its community name in the community field. If there are NEs between the GNE and ENE, you can enter up to two SNMP proxy relay addresses and community names in the fields for Relay and Relay C. When doing this, consult the following guidelines:

- If the NE is directly connected to the GNE, enter the address and community name of the GNE for Relay A.
- If this NE is connected to the GNE through other NEs, enter the address and community name of the GNE for Relay A and the address and community name of NE 1 for Relay B and NE 2 for Relay C.

The SNMP proxy directs SNMP traps in the following general order:
ENE > RELAY A > RELAY B > RELAY C > NMS. For example:

- If there is are 0 intermediate relays, the order is ENE > RELAY A (GNE) > NMS
- If there is 1 intermediate relay, the order is ENE > RELAY A (NE 1) > RELAY B (GNE) > NMS
- If there is are 0 intermediate relays, the order is ENE > RELAY A (NE 1) > RELAY B (NE 2) > RELAY C (GNE) > NMS

Step 10 Click **Apply**.

Step 11 Repeat Step 2 through Step 10 for all NEs between the GNE and ENE.

Step 12 Return to your originating procedure (NTP).

DLP-C227 Format and Enter NMS Community String for SNMP Command or Operation

Purpose	This procedure describes how to format a network management system (NMS) community string to execute the following SNMP commands for GNEs and ENEs: Get, GetBulk, GetNext, and Set.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If the SNMP "Get" (or other operation) is enabled on the ONS 15310-CL or ONS 15310-MA configured as a GNE, enter the community name assigned to the GNE in community name field on the MIB browser.

Note The community name is a form of authentication and access control. The community name of the NMS must match the community name assigned to the ONS 15310.

Step 2 If the SNMP "Get" (or other operation) is enabled for the ENE through a SOCKS proxy-enabled GNE, create a formatted string to enter in the MIB browser community name field. Refer to the following examples when constructing this string for your browser:

- Formatted community string input example 1:

```
allviews{192.168.7.4,,,net7node4}
```

  If "allviews" is a valid community name value at the proxy-enabled SNMP agent (the GNE), the GNE is expected to forward the PDU to 192.168.7.4 at Port 161. The outgoing PDU will have "net7node4" as the community name. This is the valid community name for the ENE with address 192.168.7.4.

- Formatted community string input example 2:

```
allviews{192.168.7.99,,,enter7{192.168.9.6,161,,net9node6}}
```

  If "allviews" is a valid community name value at the proxy-enabled GNE, the GNE is expected to forward the PDU to 192.168.7.99 at the default port (Port 161) with a community name of "enter7{192.168.9.6,161,,net9node6}". The system with the address 192.168.7.99 (the NE between the GNE and ENE) forwards this PDU to 192.168.9.6 at Port 161 (at the ENE) with a community name of "net9node6". The community name "enter7" is valid for the NE between the GNE and the ENE and "net9node6" is a valid community name for the ENE.

Step 3 Log into the NMS where the browser is installed to retrieve the network information from the ONS 15310.

Step 4 On this computer, go to Start and click the SNMP MIB browser application.

Step 5 In the Host and Community areas, enter the IP address of the GNE through which the ONS 15310 with the information to be retrieved can be reached.

Step 6 In the Community area, enter the community string as explained in Step 2.

Step 7 Return to your originating procedure (NTP).

DLP-C228 Provision Orderwire

Purpose	This task provisions orderwire.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the network view, click the **Provisioning > Overhead Circuits** tabs.

Step 2 Click **Create**.

Step 3 In the Overhead Circuit Creation dialog box, complete the following fields in the Circuit Attributes area:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces).
- Circuit Type—Choose either **Local Orderwire** or **Express Orderwire** depending on the orderwire path that you want to create. If regenerators are not used between nodes, you can use either local or express orderwire channels. If regenerators exist, use the express orderwire channel.
- PCM—Choose the Pulse Code Modulation voice coding and companding standard, either Mu_Law (North America, Japan) or A_Law (Europe). The provisioning procedures are the same for both types of orderwire.

Caution When provisioning orderwire for nodes that reside in a ring, do not provision a complete orderwire loop. For example, a four-node ring typically has east and west ports provisioned at all four nodes. However, to prevent orderwire loops, provision two orderwire ports (east and west) at all but one of the ring nodes.

Step 4 Click **Next**.

Step 5 In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.

Step 6 Click **Next**.

Step 7 In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.

- Port—If displayed, choose the destination port.

Step 8 Click **Finish**.

Step 9 Return to your originating procedure (NTP).

DLP-C229 Consolidate Links in Network View

Purpose	This task consolidates data communications channel (DCC), GCC, optical transport section (OTS), provisionable patchcord (PPC), and server trail links in the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note Global consolidation persists when CTC is re-launched but local consolidation does not.

Step 1 From the View menu, choose **Go to Network View**. CTC shows the link icons by default.

Step 2 Perform the following steps as needed:

- To toggle between link icons, go to Step 3.
- To consolidate all the links on the network map, go to Step 4.
- To consolidate a link or links between two nodes, go to Step 5.
- To view information about a consolidated link, go to Step 6.
- To access an individual link within a consolidated link, go to Step 7.
- To expand consolidated links, go to Step 8.
- To filter the links by class, go to Step 9.

Step 3 Right-click the network map and choose **Show Link Icons** to toggle the link icons on and off.

Step 4 To consolidate all the links on the network map (global consolidation):

a. Right-click anywhere on the network map.

b. Choose **Collapse/Expand Links** from the shortcut menu. The Collapse/Expand Links dialog window appears.

c. Select the check boxes for the link classes you want to consolidate.

d. Click **OK**. The selected link classes are consolidated throughout the network map.

Step 5 To consolidate a link or links between two nodes:

a. Right-click the link on the network map.

b. Choose **Collapse** [*link class*] **Link** from the shortcut menu, where “link class” is DCC, GCC, OTS, PPC, or server trail. The selected link type consolidates to show only one link.

Note The links consolidate by class. For example, if you select a DCC link for consolidation only the DCC links will consolidate, leaving any other link classes expanded.

Figure 19-3 shows the network view with unconsolidated DCC and PPC links.

Figure 19-3 Unconsolidated Links in the Network View

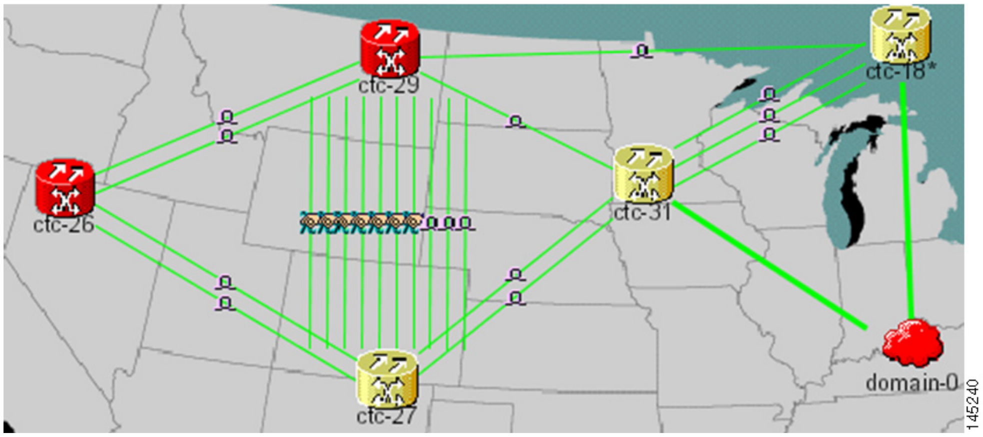


Figure 19-4 shows a network view with globally consolidated links.

Figure 19-4 Consolidated Links in the Network View

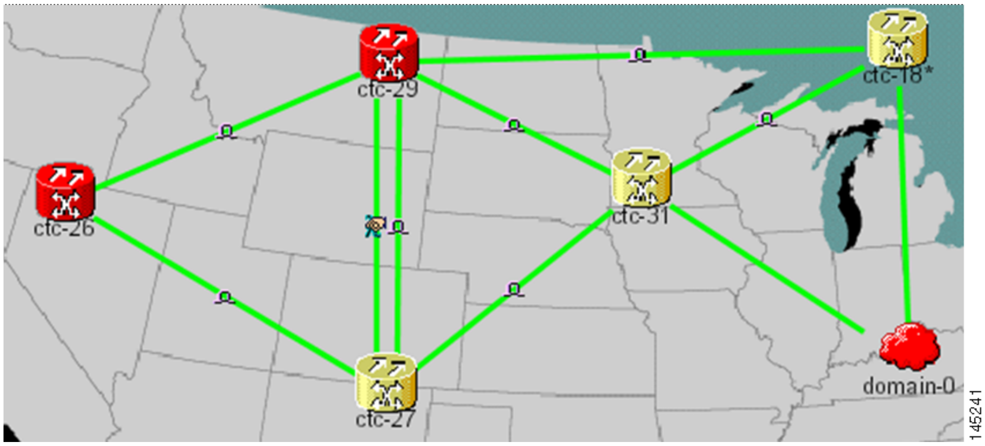
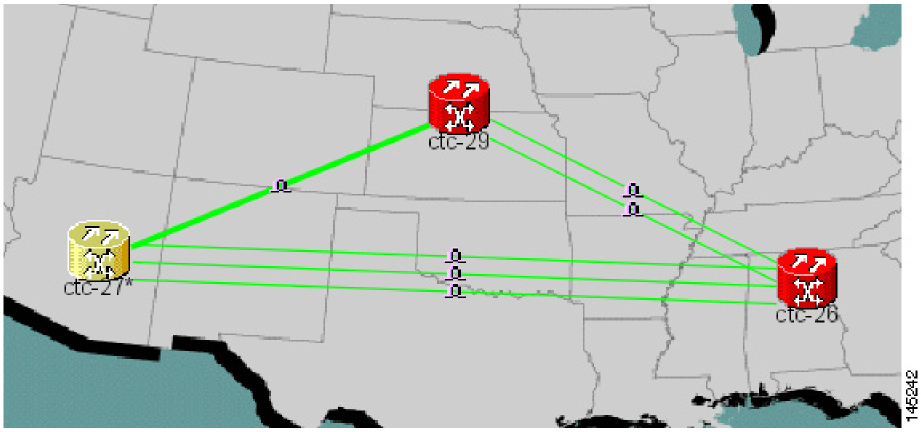


Figure 19-5 shows a network view with local DCC link consolidation between two nodes.

Figure 19-5 Network View with Local Link Consolidation



Step 6 To view information about a consolidated link, either move your mouse over the link (the tooltip displays the number of links and the link class) or single-click the link to display detailed information on the left side of the window.

Step 7 To access an individual link within a consolidated link (for example, if you need to perform a span upgrades):

a. Right-click the consolidated link. A shortcut menu appears with a list of the individual links.

b. Hover the mouse over the selected link. A cascading menu appears where you can select an action for the individual link or navigate to one of the nodes where the link is attached.

Step 8 To expand locally consolidated links, right-click the consolidated link and choose **Expand Links** from the shortcut menu.

Step 9 To filter the links by class:

a. Click the **Link Filter** button in the upper right area of the window. The Link Filter dialog appears.

The link classes that appear in the Link Filter dialog are determined by the Network Scope you choose in the network view (Table 19-2).

Table 19-2 Link Classes By Network Scope

Network Scope	Displayed Link Classes
ALL	DCC, GCC, OTS, PPC, Server Trail
DWDM	GCC, OTS, PPC
TDM	DCC, PPC, Server Trail

b. Check the check boxes next to the links you want to display.

c. Click **OK**.

Step 10 Return to your originating procedure (NTP).

DLP-C231 Adjust the Java Virtual Memory Heap Size

Purpose	This task allows you to adjust the Java Virtual Memory (JVM) heap size from the default 256 MB to the maximum of 512 MB in order to improve CTC performance.
Tools/Equipment	None
Prerequisite procedures	None
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click **Start > Settings > Control Panel**. The Windows Control Panel appears.

Step 2 Double-click **System**. The System Properties window appears.

Step 3 Click the **Advanced** tab.

Step 4 Click **Environmental Variables**. The Environmental Variables window appears.

Step 5 In the User Variables area, click **New**. The New User Variable window appears.

Step 6 Type "CTC_HEAP" in the Variable Name field.

Step 7 Type "512" in the Variable Value field.

Step 8 Click **OK**.

Step 9 Reboot your PC.

Step 10 Return to your originating procedure (NTP).

DLP-C232 Delete a Server Trail

Purpose	This task deletes a server trail.
Tools/Equipment	None
Prerequisite Procedures	NTP-C140 Create a Server Trail, page 6-55 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Deleting server trails do not impact the circuits provisioned over it as server trail is a logical link. When you delete a server trail, the circuit state becomes PARTIAL.

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

Step 2 Click the **Provisioning > Server Trails** tabs.

Step 3 Click the server trail that you want to delete.

Step 4 Click **Delete**.

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

Note You can use the server trail audit log to recreate a server trail that you may have accidentally deleted. The server trail audit log includes the following parameters:

- Server trail ID
- Peer IP address
- Circuit size
- Protection type
- Number of trails
- Starting STS/VT
- SRLG value

You can look at the audit log of the source or destination node and find the entry for the delete call. This log entry has the STS/VT path definitions on the node, peer IP address, and server trail ID. You can then look at the audit log of the peer IP address, locate the delete call for the specific server trail ID, and find the STS/VT path definitions on the node. This would provide you with the required information to recreate the server trail.

Note It is recommended that you delete one server trail at a time as the deletion of multiple trails together may cause CTC to hang and is a time consuming task.

Step 6 Return to your originating procedure (NTP).

DLP-C233 Change Line and Threshold Settings for DS-1 Ports

Purpose	This task changes line and threshold settings for DS-1 ports on the 15310-CL-CTX card and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Refer to the “Network Element Defaults” appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for DS-1 port default settings.

Step 1 In node view, double-click the 15310-CL-CTX card, DS1-28/DS3-EC1-3 card, or DS1-84/DS3-EC1-3 card where you want to change line or threshold settings.

Step 2 Click the **Provisioning > DS-1** tabs.

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, **or SONET Thresholds** subtabs.

Note If you want to modify a threshold setting, it might be necessary to click the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these subtabs by clicking in the field that you want to modify. In some fields, you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 4 and 5 for each subtab that has parameters you want to provision.

For definitions of line settings, see Table 19-3. For definitions of line threshold settings, see Table 19-4 on page 19-36. For definitions of the electrical path threshold settings, see Table 19-5 on page 19-36. For definitions of SONET threshold settings, see Table 19-6 on page 19-37.

Table 19-3 describes the values on the Provisioning > DS-1> Line tab for the DS-1 ports.

Table 19-3 Line Options for DS-1 Ports

Parameter	Description	Options
Port #	Port number.	• 1 to 21 (15310-CL-CTX, ONS 15310-CL only) • 1 to 28 (DS1-28/DS3-EC1-3; ONS 15310-MA only) • 1 to 84 (DS1-84/DS3-EC1-3; ONS 15310-MA only)
Port Name	Port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default See the "DLP-C56 Assign a Name to a Port" task on page 17-75.

Table 19-3 Line Options for DS-1 Ports (continued)

Parameter	Description	Options
Admin State	Sets the port service state unless network conditions prevent the change.	• IS—(In Service) Puts the port in service. The port service state changes to In Service and Normal (IS-NR). • IS,AINS—(In Service and Automatic In-Service) Puts the port in automatic in-service. The port service state changes to Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS). • OOS,DSBLD—(Out-of-Service and Disabled) Removes the port from service and disables it. The port service state changes to Out-of-Service and Management, Disabled (OOS-MA,DSBLD). • OOS,MT—(Out-of-Service and Maintenance) Removes the port from service for maintenance. The port service state changes to Out-of-Service and Management, Maintenance (OOS-MA,MT). **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.
Service State	Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—The port is fully operational and performing as provisioned. • OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. • OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 (default) • 1E-5

Table 19-3 Line Options for DS-1 Ports (continued)

Parameter	Description	Options
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• D4 • ESF—Extended Super Frame • Unframed • AUTO PROVISION FMT
Line Coding	Defines the DS-1 transmission coding type.	• AMI—Alternate Mark Inversion (default) • B8ZS—Bipolar 8 Zero Substitution
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 131 (default) • 132 - 262 • 263 - 393 • 394 - 524 • 525 - 655
AINS Soak	Automatic in-service soak.	• Duration of valid input signal in hh.mm after which the port is set in service by the software. • 0 to 48 hours, 15-minute increments
Provides Sync	(Display only) If checked, the card is provisioned as a NE timing reference.	• Yes (checked) • No (unchecked)
SyncMsgIn	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Yes (checked, default) • No (unchecked)
Send DoNotUse	When checked, sends a do not use (DUS) message on the S1 byte.	• Yes (checked) • No (unchecked, default)
Enable Retiming	Retiming is an option that, when enabled, removes accumulated jitter and wander from synchronous transport network payload signals.	• Yes (checked) • No (unchecked, default)

Table 19-4 describes the values on the Provisioning > DS-1> Line Thresholds tab for the DS-1 ports.

Table 19-4 Line Thresholds Options for DS-1 Ports

Parameter	Description
Port	Port number • 1 to 21 (15310-CL-CTX, ONS 15310-CL only) • 1 to 28 (DS1-28/DS3-EC1-3; ONS 15310-MA only) • 1 to 84 ((DS1-84/DS3-EC1-3; ONS 15310-MA only)
CV	Coding violations. Available for Near End only.
ES	Errored seconds. Available for Near End and Far End.
SES	Severely errored seconds. Available for Near End only.
LOSS	Number of one-second intervals containing one or more loss of signal (LOS) defects. Available for Near End only.

Table 19-5 describes the values on the Provisioning > DS-1> Elect Path Thresholds tab for the DS-1 ports.

Table 19-5 Electrical Path Threshold Options for DS-1 Ports

Parameter	Description
Port	Port number • 1 to 21 (15310-CL-CTX, ONS 15310-CL only) • 1 to 28 (DS1-28/DS3-EC1-3; ONS 15310-MA only) • 1 to 84 ((DS1-84/DS3-EC1-3; ONS 15310-MA only)
CV	Coding violations. Available for Near End and Far End.
ES	Errored seconds. Available for Near End and Far End.
SES	Severely errored seconds. Available for Near End and Far End.
SAS	Severely errored frame/alarm indication signal. Available for Near End only.
AISS	Alarm indication signal seconds. Available for Near End only.
UAS	Unavailable seconds. Available for Near End and Far End.
FC	Failure count. Available for Near End and Far End.
CSS	Controlled Slip Seconds. Available for Far End only.
ESA	Errored Seconds-A. Available for Far End only.
ESB	Errored Seconds-B.Available for Far End only.
SEFS	Severely errored framing seconds. Available for Far End only.

Table 19-6 describes the values on the Provisioning > DS-1> SONET Thresholds tab for the DS-1 ports.

Table 19-6 SONET Thresholds Options for DS-1 Ports

Parameter	Description
Port #	DS-1 ports partitioned for synchronous transport signal (STS) • 1 to 21 (15310-CL-CTX, ONS 15310-CL only) • 1 to 28 (DS1-28/DS3-EC1-3; ONS 15310-MA only) • 1 to 84 ((DS1-84/DS3-EC1-3; ONS 15310-MA only)
CV	Coding violations. Available for Near End and Far End.
ES	Errored seconds. Available for Near End and Far End.
FC	Failure count. Available for Near End and Far End.
SES	Severely errored seconds. Available for Near End and Far End.
UAS	Unavailable seconds. Available for Near End and Far End.

Note The threshold value displays after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-C234 Grant Superuser Privileges to Provisioning Users

Purpose	This task enables a provisioning user to retrieve audit logs, clear PM privileges, restore databases, and activate and revert software loads.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 In the Defaults Selector area, choose NODE > security > grantPermission.

Step 3 Click in the Default Value column for the default property you are changing and choose **Provisioning** from the drop-down list.

Note If you click **Reset** before you click **Apply**, all values will return to their original settings.

Step 4 Click **Apply**.

A pencil icon will appear next to the default name that will be changed as a result of editing the defaults file.

Note After you have activated a software load, you must close your current CTC session and restart a new CTC session for the changes to take effect.

Step 5 Return to your originating procedure (NTP).

DLP-C235 Change the OSI Routing Mode

Purpose	This task changes the OSI routing mode.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Do not complete this procedure until you confirm the role of the node within the network. It will be either an ES or IS Level 1. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Caution LSP buffers must be the same at all NEs within the network, or loss of visibility could occur. Do not modify the LSP buffers unless you are sure that all NEs within the OSI have the same buffer size.

Caution LSP buffer sizes cannot be greater than the LAP-D MTU size within the OSI area.

Step 1 In node view, click the **Provisioning** > **OSI** > **Main Setup** tabs.

Step 2 The following routing modes are available for the ONS 15310-CL and ONS 15310-MA:

Note Changing a routing mode should be carefully considered. Additional information about protocols are provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

- End System—The ONS 15310 performs OSI end system (ES) functions and relies upon an intermediate system (IS) for communication with nodes that reside within its OSI area.

  Note The End System routing mode is not available if more than one virtual router is enabled.

- Intermediate System Level 1—The ONS 15310 performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.

Step 3 Although Cisco does not recommend changing the LSP (Link State Protocol Data Unit) buffer sizes, you can change the L1 LSP Buffer Size field to change the Level 1 link state PDU buffer size.

Step 4 Return to your originating procedure (NTP).

DLP-C236 Change Line and Threshold Settings for DS-3 Ports

Purpose	This task changes the line and threshold settings for DS-3 ports on the 15310-CL-CTX card and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Refer to the "Network Element Defaults" appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for DS-3 port default settings.

Step 1 In node view, double-click the 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card where you want to change line or threshold settings.

Step 2 Click the **Provisioning > DS-3** tabs.

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, or **SONET Thresholds** subtab.

Note If you want to modify a threshold setting, it might be necessary to click the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these tabs by clicking in the field that you want to modify. In some fields, you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 4 and 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 19-7. For definitions of the line threshold settings, see Table 19-8 on page 19-41. For definitions of the electrical path threshold settings, see Table 19-9 on page 19-41. For definitions of the SONET threshold settings, see Table 19-10 on page 19-42.

Table 19-7 describes the values on the Provisioning > Line tab for the DS-3 ports.

Table 19-7 Line Options for DS-3 Ports

Parameter	Description	Options
Port #	Port number.	- 1 to 3
Port Name	Port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default. See the "DLP-C56 Assign a Name to a Port" task on page 17-75.
Admin State	Sets the port service state unless network conditions prevent the change.	- IS—Puts the port in-service. The port service state changes to IS-NR. - IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. - OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. - OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.
Service State	Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	- IS-NR—The port is fully operational and performing as provisioned. - OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. - OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. - OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
SF BER	Sets the signal fail bit error rate.	- 1E-3 - 1E-4 (default) - 1E-5

Table 19-7 Line Options for DS-3 Ports (continued)

Parameter	Description	Options
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• UNFRAMED • M13 (multiplexed DS1 to DS-3 framing) • C Bit (parity framing)
Line Coding	Defines the DS-3 transmission coding type.	• B3ZS (Bipolar 3 Zero Substitution)
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
AINS Soak	Automatic in-service soak.	• Duration of valid input signal in hh.mm after which the port is set in service by the software. • 0 to 48 hours, 15-minute increments.

Table 19-8 describes the values on the Provisioning > Line Thresholds tab for the DS-3 ports.

Table 19-8 Line Thresholds Options for DS-3 Ports

Parameter	Description
Port	Port number (display only). • 1 to 3
CV	Coding violations. Available for Near End and Far End.
ES	Errored seconds. Available for Near End and Far End.
SES	Severely errored seconds. Available for Near End and Far End.
LOSS	Number of one-second intervals containing one or more loss of signal (LOS) defects. Available for Near End and Far End.

Table 19-9 describes the values on the Provisioning > Elect Path Thresholds tab for the DS-3 ports.

Table 19-9 Electrical Path Threshold Options for DS-3 Ports

Parameter	Description
Port	(Display only) Port number. • 1 to 3
CV	Coding violations. Available for Near End (DS3 Pbit and DS3CPbit); and Far End (DS3 CPbit only).

Table 19-9 Electrical Path Threshold Options for DS-3 Ports (continued)

Parameter	Description
ES	Errored seconds. Available for Near End (DS3 Pbit and DS3CPbit); and Far End (DS3 CPbit only).
SAS	Severely errored seconds. Available for Near End, DS3 Pbit only.
SES	Severely errored seconds. Available for Near End (DS3 Pbit and DS3CPbit); and Far End (DS3 CPbit only).
UAS	Unavailable seconds. Available for Near End (DS3 Pbit and DS3CPbit); and Far End (DS3CPbit only).
AISS	Alarm indication signal seconds. Available for Near End, DS3 Pbit only.

Table 19-10 describes the values on the Provisioning > SONET Thresholds tab for the DS-3 ports.

Table 19-10 SONET Thresholds Options for DS-3 Ports

Parameter	Description
Port	Port number • 1 to 3
CV	Coding violations. Available for Near End and Far End.
ES	Errored seconds. Available for Near End and Far End.
FC	Failure count. Available for Near End and Far End.
SES	Severely errored seconds. Available for Near End and Far End.
UAS	Unavailable seconds. Available for Near End and Far End.

Note The threshold value displays after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-C237 Change Line and Threshold Settings for the EC-1 Ports

Purpose	This task changes the line and threshold settings for EC-1 ports on the 15310-CL-CTX card and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Refer to the "Network Element Defaults" appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for DS-3 port default settings.

Step 1 In node view, double-click the 15310-CL-CTX card, DS1-28/DS3-EC1-3 card, or DS1-84/DS3-EC1-3 card where you want to change line or threshold settings.

Step 2 Click the **Provisioning > EC-1** tab.

Step 3 Depending on the setting you need to modify, click the **Line** or **SONET Thresholds** tab.

Note If you want to modify a threshold setting, it might be necessary to click the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Note To modify settings on the SONET STS tab, see the "DLP-C99 Enable Intermediate-Path Performance Monitoring" task on page 17-119.

Step 4 Modify the settings found under these subtabs by clicking in the field that you want to modify. In some fields, you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 4 and 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 19-11 on page 19-43. For definitions of SONET threshold settings, see Table 19-12 on page 19-45.

Table 19-11 describes the values on the Provisioning > EC-1 > Line tab for the EC-1 ports.

Table 19-11 Line Options for EC-1 Ports

Parameter	Description	Options
Port	(Display only) Port number.	• 1 to 3
Port Name	Port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default See the "DLP-C56 Assign a Name to a Port" task on page 17-75.
Port Rate	(Display only) Port rate	• EC1.

Table 19-11 Line Options for EC-1 Ports (continued)

Parameter	Description	Options
Admin State	Sets the port service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.
Service State	Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—The port is fully operational and performing as provisioned. • OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. • OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 (default) • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
PJSTSMon#	Sets the STS that will be used for pointer justification. If set to Off, no STS is used.	• Off • 1

Table 19-11 Line Options for EC-1 Ports (continued)

Parameter	Description	Options
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
Rx Equalization	Equalizes the receive level in the ONS 15310-CL. Rx Equalization is always on and cannot be changed. This parameter is not available in the ONS 15310-MA.	• None
AINS Soak	Automatic in-service soak.	• Duration of valid input signal in hh.mm after which the port is set in service by the software • 0 to 48 hours, 15-minute increments

Table 19-12 describes the values on the Provisioning > SONET Thresholds tab for the EC-1 ports.

Table 19-12 SONET Thresholds Options for EC-1 Ports

Parameter	Description
Port	(Display only) Port number. • 1 to 3
CV	Coding violations. Available for Near End line, section, and path; Far End line and path.
ES	Errored seconds. Available for Near End line, section, and path; Far End line and path.
FC	Failure count. Available for Near End line and path; Far End line and path.
SES	Severely errored seconds. Available for Near End line, section and path; Far End Line and Path.
UAS	Unavailable seconds. Available for Near End line and path; Far End line and path.
PPJC-PDET	Positive Pointer Justification Count, STS Path Detected. Available for Near End and Far End path.
NPJC-PDET	Negative Pointer Justification Count, STS Path Detected. Available for Near End and Far End path.
PPJC-PGEN	Positive Pointer Justification Count, STS Path Generated. Available for Near End and Far End path.
NPJC-PGEN	Negative Pointer Justification Count, STS Path Generated. Available for Near End and Far End path.
PJCDIFF	Pointer Justification Count Difference (the absolute value of the difference between the total number of detected pointer justification counts and the total number of generated pointer justification counts). That is, PJCDiff is equal to (PPJC-PGEN - NPJC-PGEN) – (PPJC-PDET – NPJC-PDET). Available for Near End and Far End path.

Table 19-12 SONET Thresholds Options for EC-1 Ports (continued)

Parameter	Description
PJCS-PDET	Pointer Justification Count Seconds, STS Path Detected (PJCS-PDET) is a count of the one-second intervals containing one or more PPJC-PDET or NPJC-PDET. Available for Near End and Far End path.
PJCS-PGEN	Pointer Justification Count Seconds, STS Path Generated (PJCS-PGEN) is a count of the one-second intervals containing one or more PPJC-PGEN or NPJC-PGEN. Available for Near End and Far End path.
PSC	Protection switching count. Available for Near End line.
PSD	Protection switching duration. Available for Near End line.
PSC-W	Protection Switching Count, Working Line. Available for Near End line. **Note** Bidirectional line switched rings (BLSRs) are not supported on the ONS 15310-CL (although the ONS 15310-CL can be part of a network that contains BLSRs); therefore, the PSC-W, PSC-S, and PSC-R performance monitoring parameters do not increment.
PSD-W	Protection Switching Duration, Working Line. Available for Near End line. **Note** BLSRs are not supported on the ONS 15310-CL card (although the ONS 15310-CL can be part of a network that contains BLSRs); therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.

Step 7 Return to your originating procedure (NTP).

DLP-C238 Change Optical Port Line Settings

Purpose	This task changes the line settings for ONS 15310-CL and ONS 15310-MA optical ports. Optical ports for the ONS 15310-CL are located on the 15310-CL-CTX card; optical ports for the ONS 15310-MA are located on the CTX2500 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Refer to the "Network Element Defaults" appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for ONS 15310-CL and ONS 15310-MA port default settings.

Step 1 In node view, double-click the 15310-CL-CTX card or the CTX2500 card.

Step 2 Click the **Provisioning > Optical > Line** tabs.

Note If you want to modify a threshold setting, it might be necessary to click the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 3 Modify the settings described in Table 19-1 by clicking in the field that you want to modify. In some fields, you can choose an option from a drop-down list; in others you can type a value.

Table 19-13 Optical Port Line Settings

Parameter	Description	Options
Port #	(Display only) Port number.	• 1-1 (OC-3; OC-12;OC-48 [MA only]) • 2-1 (OC3; OC-12; OC-48 [MA only])
Port Name	Provides the ability to assign the specified port a name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-C56 Assign a Name to a Port" task on page 17-75.
Admin State	Sets the port service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

Table 19-13 Optical Port Line Settings (continued)

Parameter	Description	Options
Service State	Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—The port is fully operational and performing as provisioned. • OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. • OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 (default) • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
Provides Synch	(Display only) If checked, the card is provisioned as a NE timing reference.	• Yes (checked) • No (unchecked)
SyncMsgIn	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Yes (checked, default) • No (unchecked)
Admin SSM	Allows you to override the synchronization traceability unknown (STU) value (default setting).	• PRS: Primary Reference Source (Stratum 1) • ST2: Stratum 2 • TNC: Transit node clock • ST3E: Stratum 3E • ST3: Stratum 3 • SMC: SONET minimum clock • ST4: Stratum 4

Table 19-13 Optical Port Line Settings (continued)

Parameter	Description	Options
Send <FF> DoNotUse	When checked, sends a special DUS (0xff) message on the S1 byte.	• Yes • No
Send DoNotUse	When checked, sends a DUS message on the S1 byte.	• Yes (checked) • No (unchecked, default)
PJSTSMon #	Sets the STS that will be used for pointer justification. If set to 0 (available for the ONS 15310-CL) or OFF (available for the ONS 15310-MA), no STS is monitored. Only one STS can be monitored on each OC-N port.	• 0 or OFF (no STS used) • 1 – 12 (OC-12) • 1 – 48 (OC-48)
AINS Soak	Automatic in-service soak.	• Duration of valid input signal in hh.mm after which the card is set in service by the software • 0 to 48 hours, 15-minute increments
Type	Defines the port as SONET or SDH (15310-MA only).	• SONET • SDH
ALS Mode	Allows you to provision automatic laser shutdown	• Disable: ALS is off; the laser is not automatically shut down when traffic outages (LOS) occur. • Auto Restart: ALS is on; the laser automatically shuts down when traffic outages (LOS) occur. It automatically restarts when the conditions that caused the outage are resolved. • Manual Restart: ALS is on; the laser automatically shuts down when traffic outages (LOS) occur. However, the laser must be manually restarted when conditions that caused the outage are resolved. • Manual Restart for Test: Manually restarts the laser for testing.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

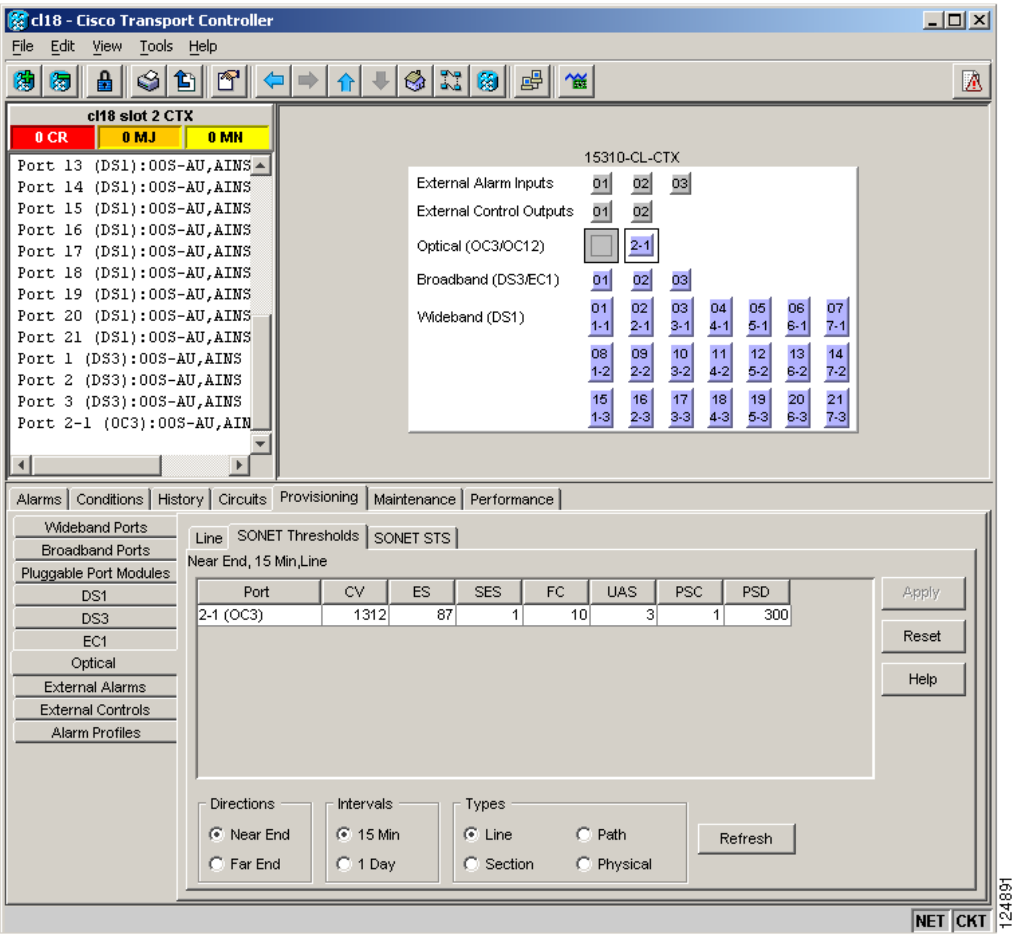
DLP-C239 Change Optical Port SONET Thresholds Settings

Purpose	This task changes SONET thresholds settings for ONS 15310-CL or ONS 15310-MA optical ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the 15310-CL-CTX card or the CTX2500 card.

Step 2 Click the **Provisioning > Optical > SONET Thresholds** tabs (Figure 19-6 and Figure 19-7).

Figure 19-6 Provisioning SONET Thresholds for the ONS 15310-CL Optical Ports



cl18 - Cisco Transport Controller

cl18 slot 2 CTX — 0 CR | 0 MJ | 0 MN

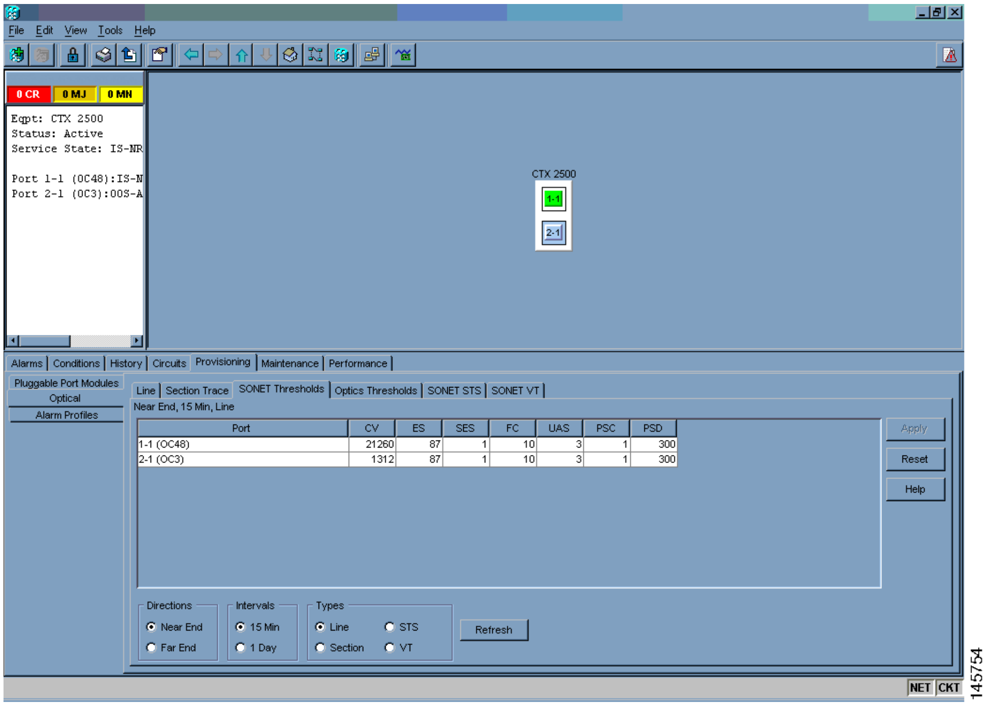
```
Port 13 (DS1):OOS-AU,AINS
Port 14 (DS1):OOS-AU,AINS
Port 15 (DS1):OOS-AU,AINS
Port 16 (DS1):OOS-AU,AINS
Port 17 (DS1):OOS-AU,AINS
Port 18 (DS1):OOS-AU,AINS
Port 19 (DS1):OOS-AU,AINS
Port 20 (DS1):OOS-AU,AINS
Port 21 (DS1):OOS-AU,AINS
Port 1 (DS3):OOS-AU,AINS
Port 2 (DS3):OOS-AU,AINS
Port 3 (DS3):OOS-AU,AINS
Port 2-1 (OC3):OOS-AU,AIN
```

Near End, 15 Min,Line

Port	CV	ES	SES	FC	UAS	PSC	PSD
2-1 (OC3)	1312	87	1	10	3	1	300

Directions: ● Near End ○ Far End
Intervals: ● 15 Min ○ 1 Day
Types: ● Line ○ Path ○ Section ○ Physical

Figure 19-7 Provisioning SONET Thresholds for the ONS 15310-MA Optical Ports


File Edit View Tools Help
0 CR
0 MJ
0 MN
CTX 2500
1-1
2-1
Alarms | Conditions | History | Circuits | Provisioning | Maintenance | Performance
Pluggable Port Modules
Optical
Alarm Profiles
Line | Section Trace | SONET Thresholds | Optics Thresholds | SONET STS | SONET VT
Apply
Reset
Help
Refresh
NET CKT
145754

```
Eqpt: CTX 2500
Status: Active
Service State: IS-NR

Port 1-1 (OC48):IS-N
Port 2-1 (OC3):OOS-A
```

Near End, 15 Min, Line

Port	CV	ES	SES	FC	UAS	PSC	PSD
1-1 (OC48)	21260	87	1	10	3	1	300
2-1 (OC3)	1312	87	1	10	3	1	300

Directions: ● Near End ○ Far End
Intervals: ● 15 Min ○ 1 Day
Types: ● Line ○ STS ○ Section ○ VT

Note If you want to modify a threshold setting, it might be necessary to click the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 3 Modify the settings described in Table 19-14 by clicking in the field that you want to modify. In some fields, you can choose an option from a drop-down list; in others you can type a value.

Table 19-14 Optical Port SONET Thresholds Options

Parameter	Description
Port	Port number • 1-1 (OC-3 or OC-12 for the ONS 15310-CL; OC-3, OC-12, or OC-48 for the ONS 15310-MA) • 2-1 (OC-3 or OC-12 for the ONS 15310-CL; OC-3, OC-12, or OC-48 for the OS 15310-MA)
CV	Coding violations. Available for Line, Section, or Path (Near and Far End).
ES	Errored seconds. Available for Line, Section, or Path (Near and Far End).
FC	Failure count. Available for Line and Path (Near End or Far End).
SES	Severely errored seconds. Available for Line, Section, and Path (Near End and Far End).
UAS	Unavailable seconds. Available for Line and Path (Near End and Far End).
PPJC-PDET	Positive Pointer Justification Count, STS Path Detected. Available for Line (Near End and Far End).

Table 19-14 Optical Port SONET Thresholds Options (continued)

Parameter	Description
NPJC-PDET	Negative Pointer Justification Count, STS Path Detected. Available for Line (Near End and Far End).
PPJC-PGEN	Positive Pointer Justification Count, STS Path Generated. Available for Line (Near End and Far End).
NPJC-PGEN	Negative Pointer Justification Count, STS Path Generated. Available for Line (Near End and Far End).
PJCDIFF	Pointer Justification Count Difference is the absolute value of the difference between the total number of detected pointer justification counts and the total number of generated pointer justification counts. That is, PJCDiff is equal to (PPJC-PGEN - NPJC-PGEN) – (PPJC-PDET – NPJC-PDET). Available for Path (Near End and Far End).
PJCS-PDET	Pointer Justification Count Seconds, STS Path Detected (PJCS-PDET) is a count of the one-second intervals containing one or more PPJC-PDET or NPJC-PDET. Available for Path (Near End and Far End).
PJCS-PGEN	Pointer Justification Count Seconds, STS Path Generated (PJCS-PGEN) is a count of the one-second intervals containing one or more PPJC-PGEN or NPJC-PGEN. Available for Path (Near End and Far End).
PSC	Protection Switching Count (Line). Available for Line (Near End and Far End).
PSD	Protection Switching Duration (Line). Available for Line (Near End and Far End).
PSC-W	Protection Switching Count, Working Line. Available for Line (Near End and Far End). **Note** BLSRs are not supported on the ONS 15310-CL (although the ONS 15310-CL can be part of a network that contains BLSRs); therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.
PSD-W	Protection Switching Duration, Working Line. Available for Line (Near End and Far End). **Note** BLSRs are not supported on the ONS 15310-CL (although the ONS 15310-CL can be part of a network that contains BLSRs); therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-C241 Edit Path Protection Dual-Ring Interconnect Circuit Hold-Off Timer

Purpose	This task changes the amount of time a path selector switch is delayed for circuits routed on a path protection dual-ring interconnect (DRI) topology. Setting a switch hold-off time (HOT) prevents unnecessary back and forth switching when a circuit is routed through multiple path protection selectors.
Tools/Equipment	None
Prerequisite Procedures	NTP-C31 Provision Path Protection Nodes, page 5-10 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Cisco recommends that you set the DRI port HOT value to zero and the circuit path selector HOT value to a number equal to or greater than zero.

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

Step 2 Click the **Circuits** tab.

Step 3 Click the path protection circuit you want to edit, then click **Edit**.

Step 4 In the Edit Circuit window, click the **Path Protection Selectors** tab.

Step 5 Create a hold-off time for the circuit source and destination ports:

a. In the Holder Off Timer area, double-click the cell of the circuit source port (top row), then type the new hold-off time. The range is 0 to 10,000 ms in increments of 100.

b. In the Hold-Off Timer area, double-click the cell of the circuit destination port (bottom row), then type the hold-off time entered in Step a.

Step 6 Click **Apply**, then close the Edit Circuit window by choosing **Close** from the File menu.

Step 7 Return to your originating procedure (NTP).

DLP-C242 Create a 1+1 Protection Group for the ONS 15310-MA

Purpose	This task creates a 1+1 protection group for ONS 15310-MA optical ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-C130 Manage Pluggable Port Modules, page 10-3 (optional)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	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 CTX2500 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 CTX2500 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 CTX2500 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 CTX2500 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 CTX2500.
- 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**.

Step 9 Return to your originating procedure (NTP).

DLP-C243 Create an Optimized 1+1 Protection Group for the ONS 15310-MA

Purpose	This task creates an optimized 1+1 protection group for ONS 15310-MA optical ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-C130 Manage Pluggable Port Modules, page 10-3 (optional)
Required/As Needed	As needed; consult your network administrator before using this feature.
Onsite/Remote	Onsite or remote
Security Level	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 CTX2500 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 CTX2500 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 CTX2500 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 CTX2500 ports. As necessary, complete the "NTP-C130 Manage Pluggable Port Modules" procedure on page 10-3 to make PPM changes.

Step 3 Change the port type from SONET to SDH for each applicable port where you want to provision a 1+1 optimized protection group:

a. In node view, double-click the applicable CTX2500.

b. Click the **Provisioning > Line** tabs.

c. In the Type column next to port, choose **SDH** from the drop-down list and click **Apply**.

Step 4 In node view, click the **Provisioning** > **Protection** tabs.

Step 5 In the Protection Groups area, click **Create**.

Step 6 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 Optimized** from the drop-down list.
- Protect Port—Choose the protect port from the drop-down list. The list displays the available optical ports. If the CTX2500s are not provisioned for SDH, no ports appear in the drop-down list.

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

Step 8 Complete the remaining fields:

- Reversion time—If Revertive is checked, choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the primary channel is automatically renamed as secondary and the secondary channel is renamed as primary. The reversion timer starts after conditions causing the switch are cleared.
- Verification guard time—Choose the verification guard time from the drop-down list. The range is 500ms to 1s. A verification guard timer is used to ensure the acceptance of a Force switch command from the far-end node. When the Force command is received, if no Lockout is present or if Secondary section is not in a failed state, then the outgoing K1 byte is changed to indicate Force and the verification guard timer is started. If a Force switch command is not acknowledged by the far-end within the verification guard timer duration, then the Force command is cleared.
- Recovery guard time—Choose the recovery guard time from the drop-down list. The range is 0s to 10s. The default is 1 second. A recovery guard timer is used for preventing rapid switches due to signal degrade (SD) or signal failure (SF) failures. After the SD/SF failure is cleared on the line, a recovery guard timer is started. Recovery guard time is the amount of time elapsed before the system declares that a condition is cleared after the detection of an SD/SF failure.
- Detection guard time—Choose the detection guard time from the drop-down list. The range is 0s to 5s. The default is 1 second. The detection guard timer is started after detecting an SD, SF, loss of signal (LOS), loss of frame (LOF), or alarm indication signal–line (AIS-L) failure. Detection guard time is the amount of time elapsed before a traffic switch is initiated to a standby port after the detection of an SD, SF, LOS, LOF, or AIS-L failure on the active port.

Step 9 Click **OK**.

Step 10 Return to your originating procedure (NTP).

DLP-C244 Modify an Optimized 1+1 Protection Group for the ONS 15310-MA

Purpose	This task modifies an optimized 1+1 protection group for ONS 15310-MA optical ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-C243 Create an Optimized 1+1 Protection Group for the ONS 15310-MA, page 19-55 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 In the Protection Groups area, click the optimized 1+1 protection group you want to modify.

Step 3 In the Selected Group area, modify the following as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.

- Reversion time—If Revertive is checked, choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the primary channel is automatically renamed as secondary and the secondary channel is renamed as primary.
- Verification guard time—Choose the verification guard time from the drop-down list. The range is 500ms to 1s. A verification guard timer is used to ensure the acceptance of a Force switch command from the far-end node. When the Force command is received, if no Lockout is present or if the Secondary section is not in a failed state, then the outgoing K1 byte is changed to indicate Force and the verification guard timer is started. If a Force user command is not acknowledged by the far-end within the verification guard timer duration, then the Force command is cleared.
- Recovery guard time—Choose the recovery guard time from the drop-down list. The range is 0s to 10s. The default is 1 second. A recovery guard timer is used for preventing rapid switches due to signal degrade (SD) or signal failure (SF) failures. After the SD/SF failure is cleared on the line, a recovery guard timer is started. Recovery guard time is the amount of time elapsed before the system declares that a condition is cleared after the detection of an SD/SF failure.
- Detection guard time—Choose the detection guard time from the drop-down list. The range is 0s to 5s. The default is 1 second. The detection guard timer is started after detecting an SD, SF, loss of signal (LOS), loss of frame (LOF), or line alarm indication signal (AIS-L) failure. Detection guard time is the amount of time elapsed before a traffic switch is initiated to a standby port after the detection of an SD, SF, LOS, LOF, or AIS-L failure on the active port.

Step 4 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-C245 Modify a 1:1 Protection Group for the ONS 15310-MA

Purpose	This task modifies a 1:1 protection group for electrical (DS1-28/DS3-EC1-3 or DS1-84/DS3-EC1-3) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 In the Protection Groups area, click the 1:1 protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—As needed, type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time drop-down list. Uncheck if you do not want traffic to revert.

- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-C248 Mount a Single ONS 15310-MA in a Rack

Purpose	This task allows one person to mount the MA shelf assembly in a rack.
Tools/Equipment	#12-24 mounting screws (4) #10-32 ear mounting screws (8) #2 Phillips screwdriver Universal mounting ear 19-inch-rack mounting ear 23-inch-rack mounting ear Fuse and alarm panel, if not installed
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Mounting the ONS 15310-MA in a rack requires a minimum of 10.5 inches of vertical rack space, including the space needed for the standard cable management bracket. If the extended cable management bracket is used, 12.25 inches is required.

Note To install the shelf assembly justified right, secure the universal mounting ear to the right side of the shelf assembly and the appropriate mounting ear for your rack size (19-inch or 23-inch) on the left side. To install the shelf assembly justified left, secure the universal mounting ear to the left side of the shelf assembly and the appropriate mounting ear for your rack size on the right side.

Step 1 Verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel has not been installed, you must install one according to manufacturer instructions. A fuse panel with two fuses per shelf (amperage depends on the fuse and alarm panel you are using) is required for Power A and B feeds.

Caution Maximum amperage rating of the fuse is determined by the rated ampacity of the selected power cable (refer to manufacturer’s instructions). The fuse rating should not exceed 20 A.

Step 2 Align the screw holes on the desired mounting ear with the screw holes at the front of the shelf assembly, and install four #10-32 screws.

Step 3 Repeat Step 2 for the other mounting ear.

Step 4 Lift the shelf assembly to the desired rack position.

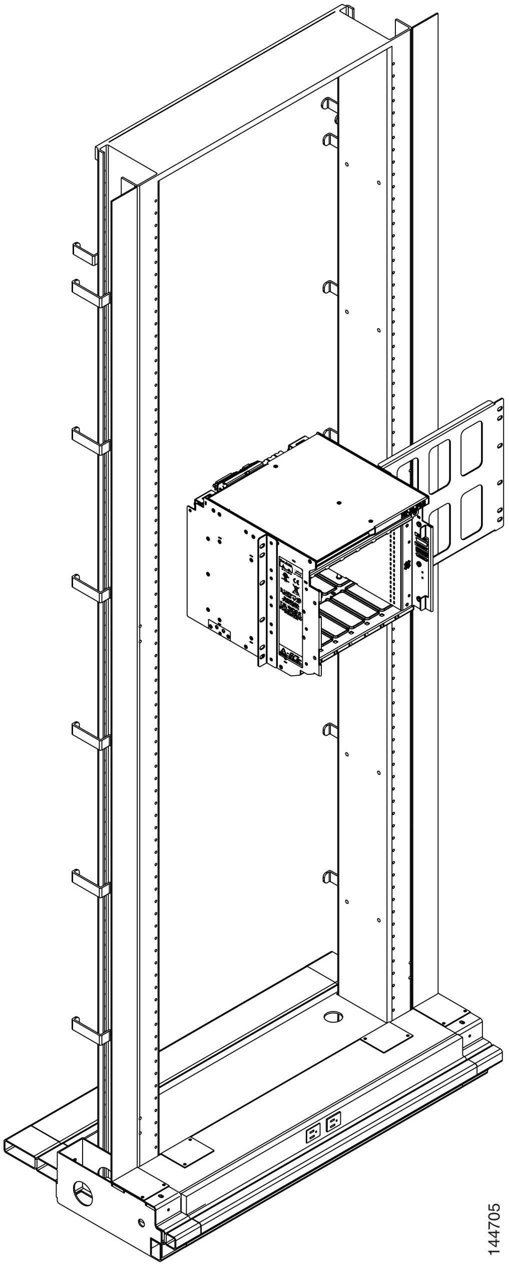
Step 5 Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 6 Using the Phillips screwdriver, install one #12-24 mounting screws in each side of the assembly.

Step 7 When the shelf assembly is secured to the rack, install the remaining two mounting screws through the rack into the shelf assembly.

Figure 19-8 shows a single ONS 15310-MA being mounted in a rack.

Figure 19-8 Mounting a Single, Left-Justified ONS 15310-MA in a Rack



Note If you want to install a tie-down bar on the rack, be sure to leave 1 RU spacing between the ONS 15310-MA and any adjacent equipment you plan to install on the rack. This will provide adequate space for the tie-down bar and cabling.

Step 8 Return to your originating procedure (NTP).

DLP-C249 Mount Dual ONS 15310-MA Shelf Assemblies in a Rack

Purpose	This task simultaneously installs two shelf assemblies in a rack.
Tools/Equipment	#2 Phillips screwdriver #12-24 mounting screws (4) #10-32x0.31 length screws (7) #10-32x0.375 length ear mounting screws (9) #10-32 nut (1) Universal mounting ears (2) Dual-assembly plate
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel is not present, you must install one according to manufacturer instructions. A fuse panel with two fuses per shelf (amperage depends on the fuse and alarm panel you are using) is required for Power A and B feeds.

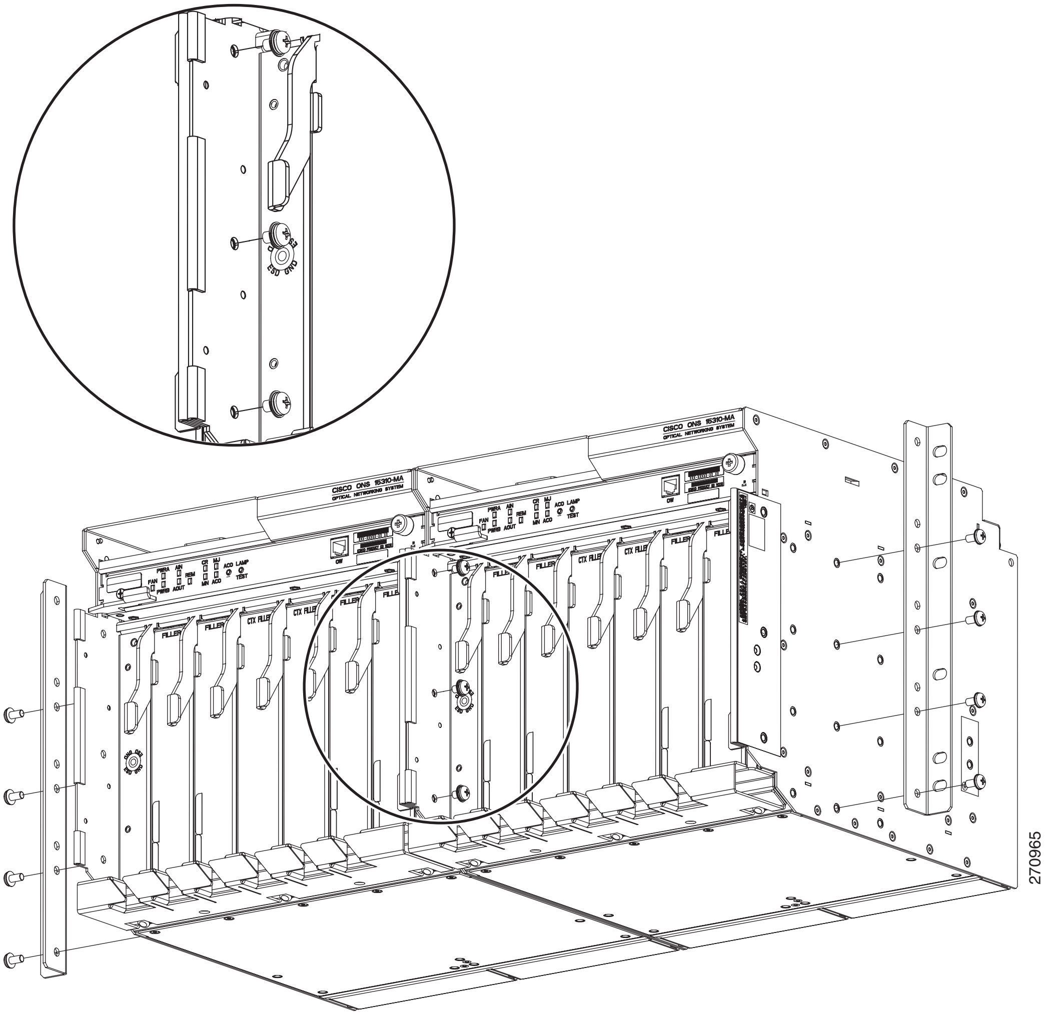
⚠ **Caution** Maximum amperage rating of the fuse is determined by the rated ampacity of the selected power cable (refer to manufacturer’s instructions). The fuse rating should not exceed 20 A.

Step 2 Align the screw holes on a universal mounting ear with the screw holes at the left front of the shelf assembly, and install four #10-32x0.375 screws.

Step 3 Align the screw holes on a universal mounting ear with the screw holes at the right front of the other shelf assembly, and install four #10-32x0.375 screws.

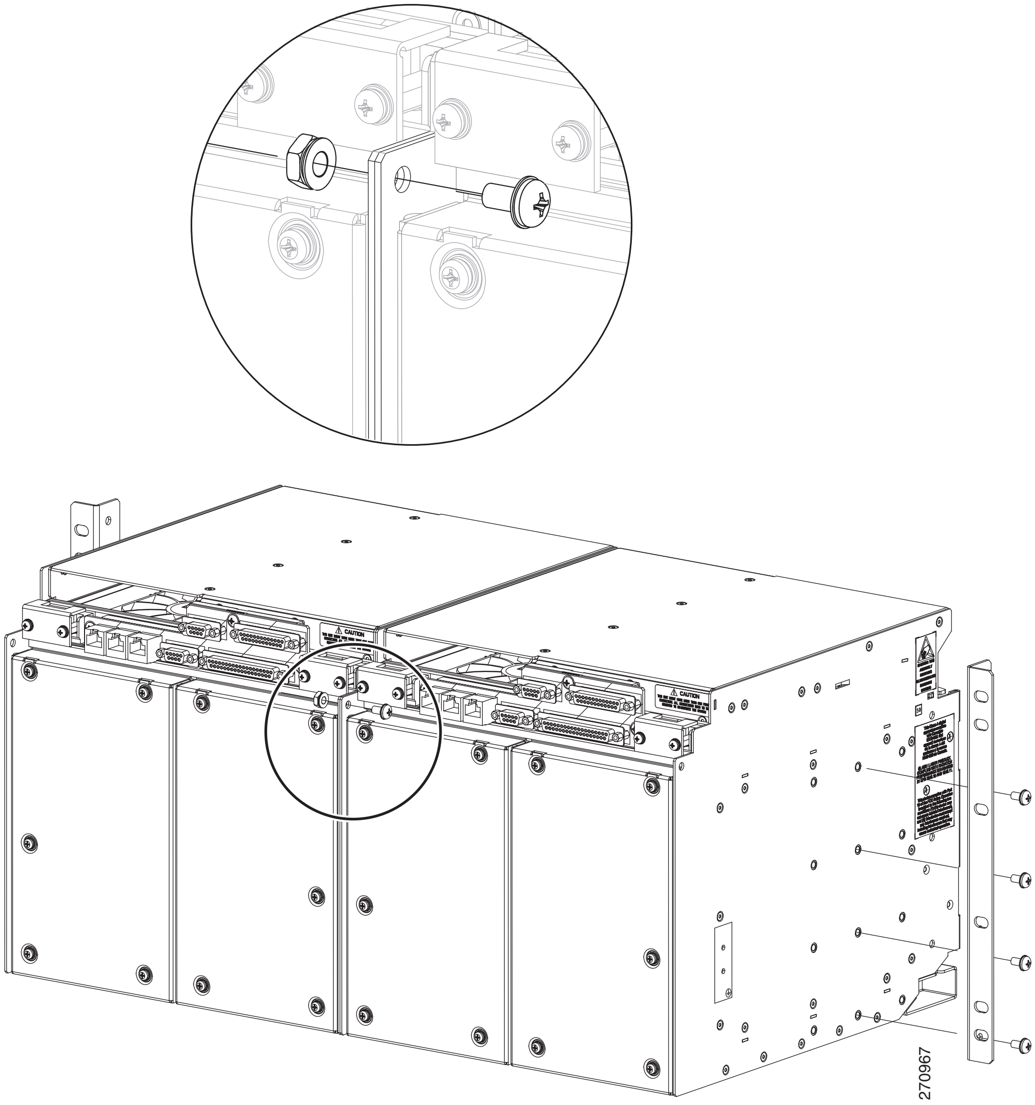
Step 4 Align the two shelves on the front, common lateral side. Using the Phillips screwdriver, install three mounting screws; #10-32x0.31 length. Figure 19-9 shows the two shelves aligned along a common lateral side.

Figure 19-9   ONS 15310-MA Shelves Aligned along a Common Lateral Side



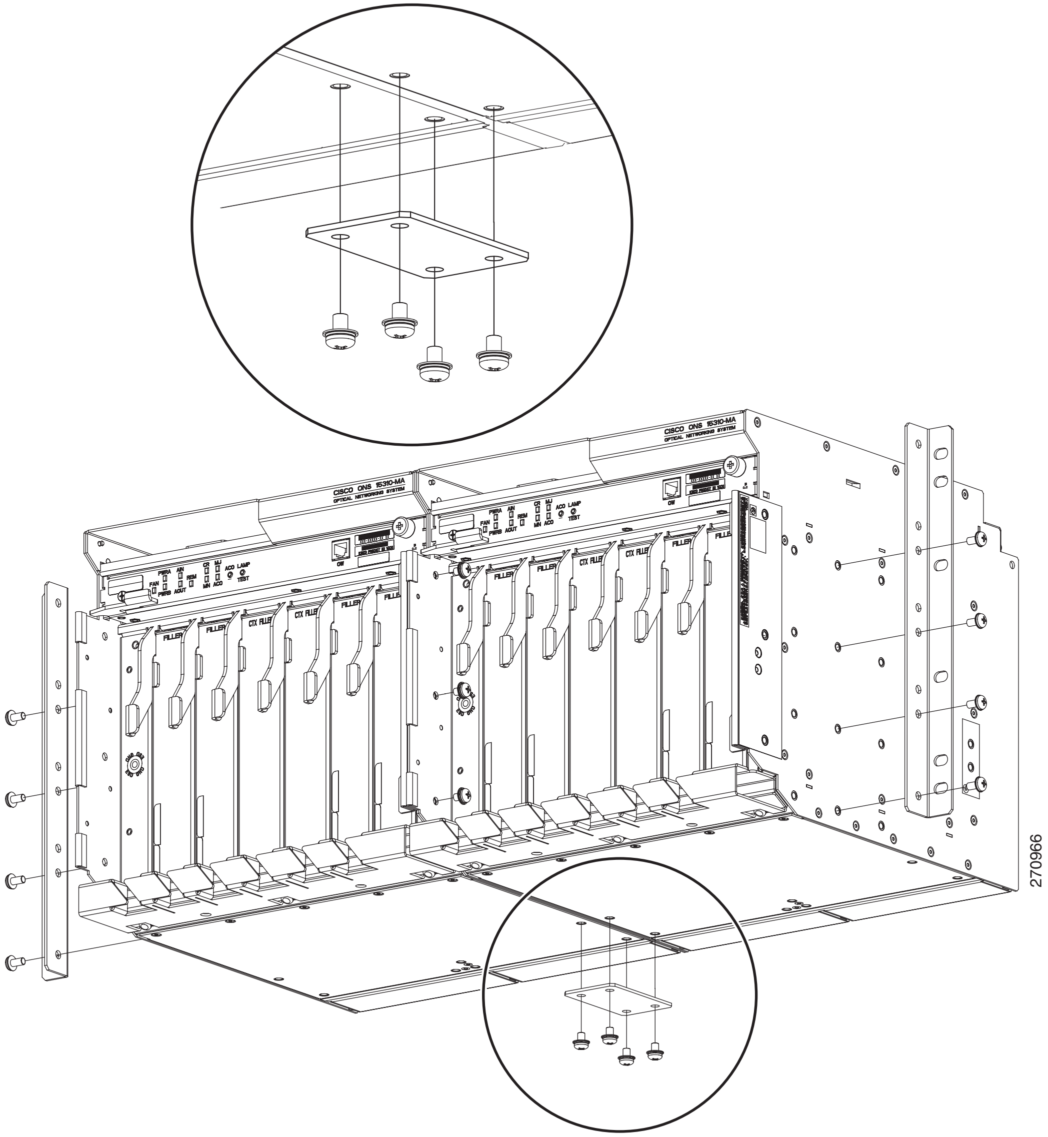
Step 5   Install screws #10-32x0.375 length with its #10-32 nut on the rear common lateral side as shown in Figure 19-10.

Figure 19-10 ONS 15310-MA Shelves Aligned on the Rear Common Lateral Side



Step 6 Install the dual-assembly plate at the bottom of the shelf assembly by aligning it with four screws #10-32x0.31 length as shown in Figure 19-11.

Figure 19-11 Dual-Assembly Plate aligned to the ONS 15310-MA Shelf



Step 7 Lift the dual-shelf assembly to the desired rack position.

Step 8 Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 9 Using the Phillips screwdriver, install one #12-24 mounting screws in each side of the assembly.

Step 10 When the shelf assembly is secured to the rack, install the remaining two mounting screws through the rack into the shelf assembly.

Note If you want to install a tie-down bar on the rack, be sure to leave 1 RU spacing between the ONS 15310-MA and any adjacent equipment you plan to install on the rack. This will provide adequate space for the tie-down bar and cabling.

Step 11 Repeat the task with the remaining ONS 15310-MA nodes.

Step 12 Return to your originating procedure (NTP).

DLP-C250 Connect the Office Ground to the ONS 15310-MA

Purpose	This task connects ground to the ONS 15310-MA shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Screws Ground cable, #6 AWG, copper conductors, 194°F [90°C]) #6 AWG dual-hole, 5/8-in. (1.59-cm) spaced grounding lug 10-32 screws Crimp tool Wire strippers Wire cutter
Prerequisite Procedures	DLP-C248 Mount a Single ONS 15310-MA in a Rack, page 19-58
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify that the office ground cable (#6 AWG stranded) is connected to the top of the rack according to local site practice.

Note Additional ground cables may be added depending on the local site practice. The ONS 15310-MA is designated for a Common Bonding Network (CBN) only, according to definitions in section 9.3 of GR1089 issue 4.

Step 2 Ensure to remove paint and other nonconductive coatings from the surfaces between the shelf ground and the rack frame ground posts. Clean the mating surfaces and apply an appropriate antioxidant compound to the bare conductors.

Step 3 Locate the ground connection points, which are located on left, right, and bottom of the ONS 15310-MA shelf assembly.

Figure 19-12 and Figure 19-13 show the ground locations on the ONS 15310-MA.

Figure 19-12 Ground Holes on the Bottom of the ONS 15310-MA Shelf Assembly

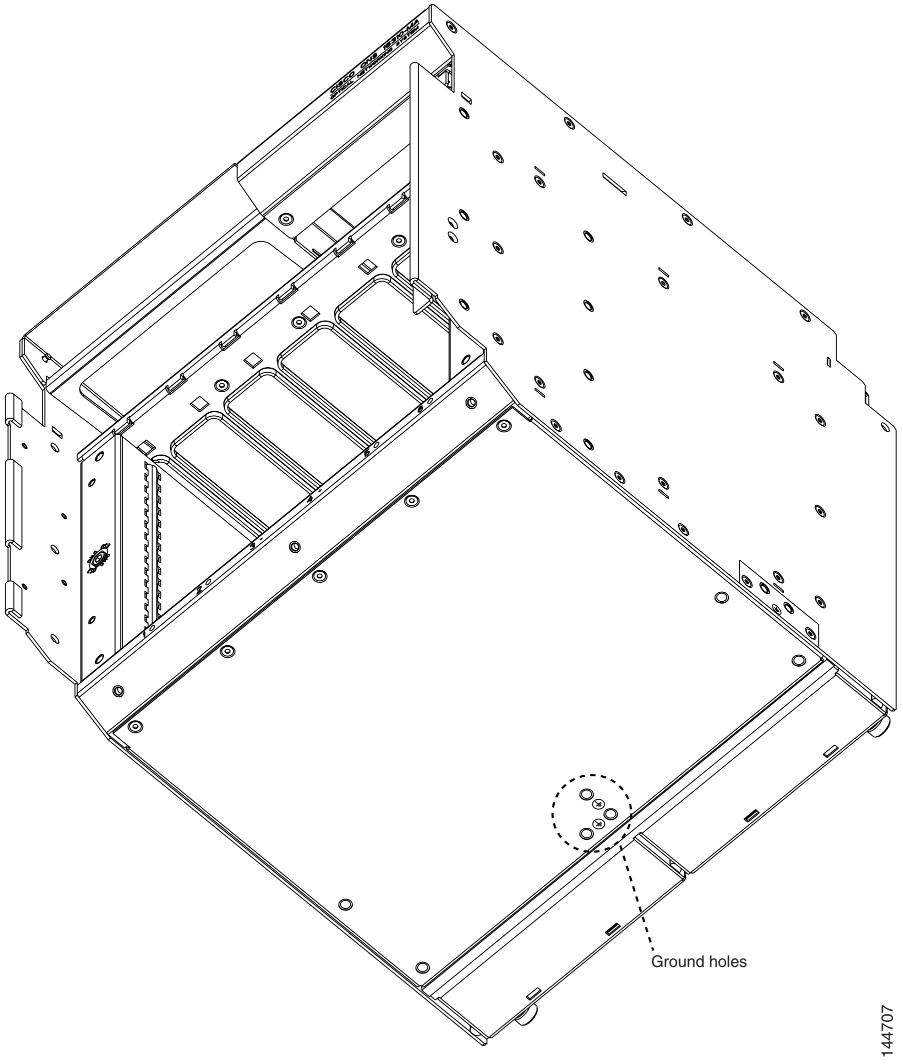
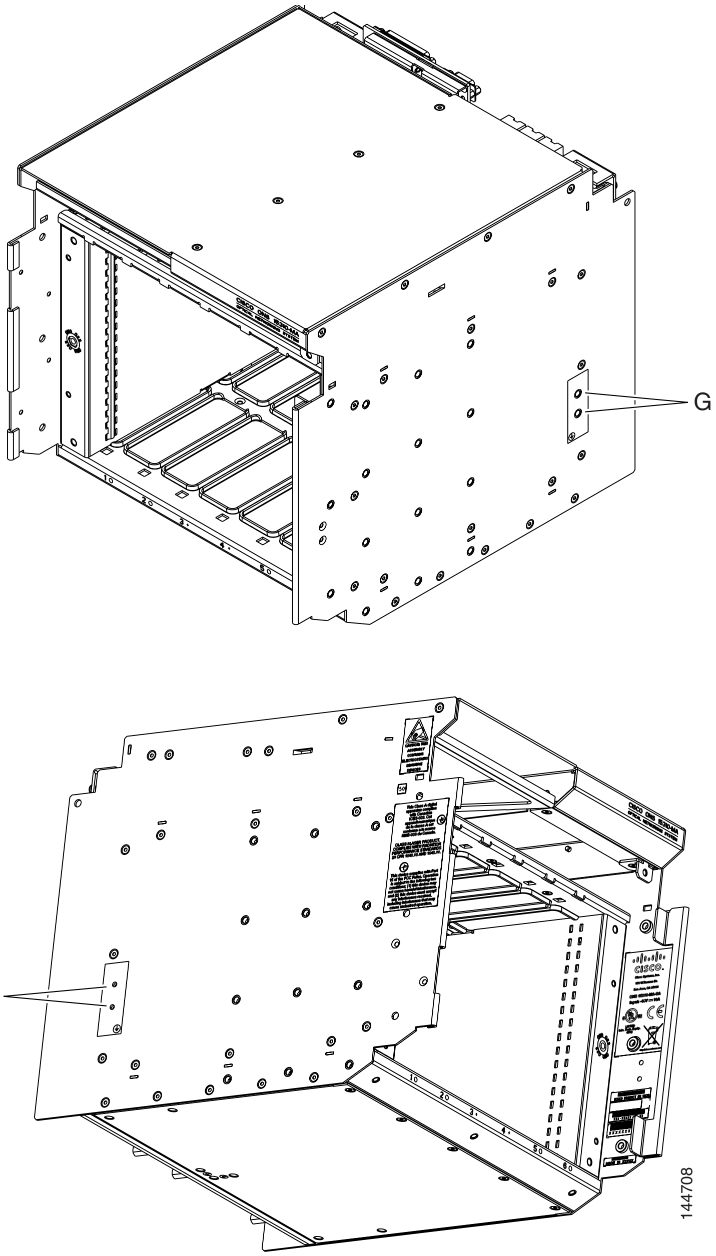


Figure 19-13 Ground Holes on the Left and Right Sides of the ONS 15310-MA Shelf Assembly



Step 4 Using a wire stripper, strip 0.875 in. (2.22 cm) from the end of a #6 AWG ground cable.

Step 5 Crimp the two-hole lug to the #6 AWG ground cable.

Step 6 Line up the holes on the lug with the holes on the ground connection point. Use two 10-32 screws to attach the lug to the ground connection point.

Step 7 Attach the other end of the shelf ground cable to the rack.

Step 8 Return to your originating procedure (NTP).

DLP-C251 Connect Office Power to the ONS 15310-MA

Purpose	This task connects office power to the ONS 15310-MA shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Wire wrapper Wire cutters Wire strippers Fuse and alarm panel Power cable (from fuse and alarm panel to assembly), #12 AWG, stranded (41 strands, 0.010 in. [0.025 cm]) Listed pressure terminal connectors such as ring and fork types; 12 AWG, stranded (41 strands, 0.010 in. [0.025 cm])
Prerequisite Procedures	DLP-C250 Connect the Office Ground to the ONS 15310-MA, page 19-65
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note If you encounter problems with the power supply, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Step 1 Connect the office power according to the fuse panel engineering specifications.

Step 2 Measure and cut the cables as needed to reach the ONS 15310-MA from the fuse panel.

Step 3 Dress the power cabling according to local site practice.

Step 4 Remove or loosen the power terminal screws on the ONS 15310-MA. To avoid confusion, label the cables connected to the BAT1/RET1 (A) power terminals as 1, and the cables connected to the BAT2/RET2 (B) power terminals as 2.

Note Use only pressure terminal connectors, including ring, fork, and dual-lug types, when terminating the battery, battery return, and frame ground conductors.

Note The battery return connection (+48Vdc) can be treated as DC-I , as defined in Telcordia GR-1089-CORE Issue 4. Connect the battery return (+48Vdc) to ground at the power source level.

Caution Before you make any crimp connections, coat all bare conductors (battery, battery return, and frame ground) with an appropriate antioxidant compound. Bring all unplated connectors, braided strap, and bus bars to a bright finish, then coat with an antioxidant before you connect them. You do not need to prepare tinned, solder-plated, or silver-plated connectors and other plated connection surfaces, but always keep them clean and free of contaminants.

Note When terminating power, return, and frame ground, do not use soldering lug, screwless (push-in) connectors, quick-connect, or other friction-fit connectors.

Step 5 Strip away 0.2 in. of insulation at one end of two 12 AWG wires.

Step 6 Crimp the lugs onto the ends of all power leads.

Step 7 Using a Phillips screwdriver, remove the two screws that hold the plastic covers over the A and B power terminal strips. (There are two screws on each for A and B power.)

Step 8 Terminate the return 1 lead to the RET1 backplane terminal. Use oxidation-prevention grease to keep connections noncorrosive.

Step 9 Terminate the negative 1 lead to the negative BAT1 backplane power terminal. Use oxidation prevention grease to keep connections noncorrosive.

Step 10 If you use redundant power leads, terminate the return 2 lead to the positive RET2 terminal on the ONS 15310-MA. Terminate the negative 2 lead to the negative BAT2 terminal on the ONS 15310-MA. Use oxidation-preventative grease to keep connections noncorrosive.

Step 11 Replace and tighten the screws that hold the plastic covers over the A and B power terminal strips.

Step 12 Return to your originating procedure (NTP).

DLP-C252 Turn On and Verify Office Power to the ONS 15310-MA

Purpose	This task verifies the chassis LED activity and measures the DC power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	DLP-C250 Connect the Office Ground to the ONS 15310-MA, page 19-65 DLP-C251 Connect Office Power to the ONS 15310-MA, page 19-68
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Using a voltmeter, verify the office battery and ground at the following points on the fuse and alarm panel:

a. To verify the power, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the A-side connection and verify that it is between -44 VDC and -52 VDC. Place the red test lead on the B-side connection and verify that it is between -44 VDC and -52 VDC.

Note The voltages -44 VDC and -52 VDC are the minimum and maximum voltages required to power the chassis. The nominal steady-state voltage is -48 VDC.

b. To verify the ground, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the A-side return ground and verify that no voltage is present. Place the red test lead on the B-side return ground and verify that no voltage is present.

Step 2 According to site practice, insert a fuse into the fuse position.

Step 3 Using a voltmeter, verify the shelf for –48 VDC battery and ground:

a. To verify the A-side of the shelf, place the black lead of the voltmeter to the frame ground. Place the red test lead to the BAT1 (A-side battery connection) red cable. Verify that it reads between –44 VDC and –52 VDC. Then place the red test lead of the voltmeter to the RET1 (A-side return ground) black cable and verify that no voltage is present.

b. To verify the B-side of the shelf, place the black test lead of the voltmeter to the frame ground. Place the red test lead to the BAT2 (B-side battery connection) red cable. Verify that it reads between –44 VDC and –52 VDC. Then place the red test lead of the voltmeter to the RET2 (B-side return ground) black cable and verify that no voltage is present.

Step 4 Return to your originating procedure (NTP).

DLP-C253 Install External Alarm Cables on the ONS 15310-MA

Purpose	This task installs alarm cables on the ONS 15310-MA so that you can provision external (environmental) alarms and controls.
Tools/Equipment	Alarm In cable, unshielded cable terminated with a DB-37 connector
	Alarm Out cable, unshielded cable terminated with a DB-25 connector
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the alarm cable terminated with a DB-37 connector into the ALARM IN port at the rear of the ONS 15310-MA.

Step 2 Plug the other end of the cable into the alarm-collection equipment according to local site practice.

Step 3 Plug one end of the alarm cable terminated with a DB-25 connector into the ALARM OUT port at the rear of the ONS 15310-MA.

Step 4 Plug the other end of the cable into the alarm-collection equipment according to local site practice.

Step 5 To define the 32 external alarm inputs and 8 external alarm outputs using CTC, see the "NTP-C63 Provision External Alarms and Controls" procedure on page 9-8. Table 19-15 shows the default input alarm pinouts and the corresponding alarm numbers assigned to each port. Table 19-16 shows the default output alarm pinouts and the corresponding alarm numbers assigned to each port. Refer to these tables when connecting alarm cables to the ONS 15310-MA.

Table 19-15 Default Alarm Pin Assignments—Inputs

DB-37 Pin Number	Function	DB-37 Pin Number	Function
1	Alarm 1	20	Alarm 18
2	Alarm 2	21	Alarm 19
3	Alarm 3	22	Alarm 20
4	Alarm 4	23	Alarm 21
5	Alarm 5	24	Alarm 22
6	Alarm 6	25	Alarm 23
7	Alarm 7	26	Alarm 24
8	Alarm 8	27	Common 17–24
9	Common 1–8	28	Alarm 25
10	Alarm 9	29	Alarm 26
11	Alarm 10	30	Alarm 27
12	Alarm 11	31	Alarm 28
13	Alarm 12	32	Alarm 29
14	Alarm 13	33	Alarm 30
15	Alarm 14	34	Alarm 31
16	Alarm 15	35	Alarm 32
17	Alarm 16	36	Common 25–32
18	Common 9–16	37	N/C
19	Alarm 17	—	—

Table 19-16 Default Alarm Pin Assignments—Outputs

DB-25 Pin Number	Function	DB-25 Pin Number	Function
1	Out 1+	14	Out 2+
2	Out 1–	15	Out 2–
3	—	16	Out 3+
4	—	17	Out 3–
5	—	18	Out 4+
6	—	19	Out 4–
7	—	20	Out 5+
8	—	21	Out 5–
9	—	22	Out 6+
10	—	23	Out 6–
11	—	24	Out 7+
12	Out 8+	25	Out 7–
13	Out 8–	—	—

Step 6 Return to your originating procedure (NTP).

DLP-C254 Install Timing Cables on the ONS 15310-MA

Purpose	This task installs timing cables so that you can provide building integrated timing supply (BITS) timing to the ONS 15310-MA.
Tools/Equipment	BITS timing port cable, CAT-3/CAT-5 terminated with DB-9 connector
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the timing cable into the BITS 1 port at the rear of the ONS 15310-MA.

Step 2 Plug the other end of the cable into the BITS clock according to local site practice. Table 19-17 shows the BITS cable pin assignments.

Table 19-17 BITS Cable Pin Assignments

DSub-9 Pin Number	Function
1	BITS Output+
2	BITS Output–
3	—
4	—
5	—
6	BITS Input+
7	BITS Input–
8	—
9	—

Step 3 Repeat Steps 1 and 2 for the BITS 2 port.

Note For more detailed information about timing, refer to the "Timing" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.* To set up system timing, see the "NTP-C23 Set Up Timing" procedure on page 4-11.

Step 4 Return to your originating procedure (NTP).

DLP-C255 Install the Serial Cable for TL1 Craft Interface on the ONS 15310-MA

Purpose	This task installs the serial cable for the TL1 craft interface on the ONS 15310-MA.
Tools/Equipment	Craft port serial cable, CAT-5 terminated with RJ-45
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the TL1 cable into the CRAFT port on the CTX2500 faceplate.

Step 2 Connect the other end to the PC that you want to use to access the craft.

Table 19-18 shows the serial cable pin assignments.

Table 19-18 TL1 Serial Cable Pin Assignments

RJ-45 Pin Number	Function
1	RTS
2	DTR
3	TXD
4	GND
5	GND
6	RXD
7	DSR
8	CTS

Step 3 Return to your originating procedure (NTP).

DLP-C256 Install the UDC Cable on the ONS 15310-MA

Purpose	This task installs the user data channel (UDC) cable on the ONS 15310-MA. A UDC circuit allows you to create a dedicated data channel between nodes.
Tools/Equipment	EIA/TIA-232 port cable, CAT-5 terminated with RJ-45
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the UDC cable into the UDC port at the rear of the 15310-MA.

Step 2 Connect the other end to terminating equipment, such as a 64-Kbps codirectional ITU-T G.703 equipment interface or EIA/TIA-232-compliant equipment.

Table 19-19 shows the serial cable pin assignments.

Table 19-19 UDC Cable Pin Assignments

RJ-45 Pin Number	RS-232/64K Mode
1	TX +
2	TX –
3	RX +
4	—
5	—
6	RX –
7	—
8	—

Step 3 Return to your originating procedure (NTP).

DLP-C257 Install the LAN Cable for the CTC Interface on the ONS 15310-MA

Purpose	This task installs the LAN cable to provide a 10/100 Mbps Ethernet interface for CTC and TL1 provisioning.
Tools/Equipment	Management LAN cable, CAT-5 terminated with RJ-45
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the LAN cable into the LAN port on the CTX2500 faceplate.

Step 2 Connect the other end to the PC you want to use to access CTC.

Table 19-20 shows the LAN cable pin assignments.

Table 19-20 LAN Cable Pin Assignments

RJ-45 Pin Number	Function
1	TX +
2	TX –
3	RX +
4	—
5	—

Table 19-20 LAN Cable Pin Assignments (continued)

RJ-45 Pin Number	Function
6	RX –
7	—
8	—

Step 3 Return to your originating procedure (NTP).

DLP-C258 Install CHAMP Cables for DS-1 Connection

Purpose	This task installs DS-1 cables.
Tools/Equipment	Electrical cable, terminated with a 64-pin CHAMP connector
Prerequisite Procedures	NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

Step 1 Prepare a cable terminated with a 64-pin CHAMP connector.

Table 19-21 lists the Champ connector pin assignments and the corresponding EIA connector mapping for connectors J8 and J9 on the EIA installed on the A side, and connectors J21 and J22 on the EIA installed on the B side.

Table 19-21 Champ Connector Pin Assignments—Side-A EIA, Connectors J8 and J9; Side-B EIA, Connectors J21 and J22

Signal	Pin	Signal	Pin
Ring Port 1	1	Tip Port 1	33
Ring Port 2	2	Tip Port 2	34
Ring Port 3	3	Tip Port 3	35
Ring Port 4	4	Tip Port 4	36
Ring Port 5	5	Tip Port 5	37
Ring Port 6	6	Tip Port 6	38
Ring Port 7	7	Tip Port 7	39
Ring Port 8	8	Tip Port 8	40
Ring Port 9	9	Tip Port 9	41
Ring Port 10	10	Tip Port 10	42

Table 19-21 Champ Connector Pin Assignments—Side-A EIA, Connectors J8 and J9; Side-B EIA, Connectors J21 and J22 (continued)

Signal	Pin	Signal	Pin
Ring Port 11	11	Tip Port 11	43
Ring Port 12	12	Tip Port 12	44
Ring Port 13	13	Tip Port 13	45
Ring Port 14	14	Tip Port 14	46
Ring Port 15	15	Tip Port 15	47
Ring Port 16	16	Tip Port 16	48
Ring Port 17	17	Tip Port 17	49
Ring Port 18	18	Tip Port 18	50
Ring Port 19	19	Tip Port 19	51
Ring Port 20	20	Tip Port 20	52
Ring Port 21	21	Tip Port 21	53
Ring Port 22	22	Tip Port 22	54
Ring Port 23	23	Tip Port 23	55
Ring Port 24	24	Tip Port 24	56
Ring Port 25	25	Tip Port 25	57
Ring Port 26	26	Tip Port 26	58
Ring Port 27	27	Tip Port 27	59
Ring Port 28	28	Tip Port 28	60
Unused	29	Unused	61
Unused	30	Unused	62
Unused	31	Unused	63
Unused	32	Unused	64

Table 19-22 lists the Champ connector pin assignments and the corresponding EIA connector mapping for connectors J10 and J11 on the EIA installed on the A side, and connectors J23 and J24 on the EIA installed on the B side.

Table 19-22 Champ Connector Pin Assignments—Side-A EIA, Connectors J10 and J11; Side-B EIA, Connectors J23 and J24

Signal	Pin	Signal	Pin
Ring Port 29	1	Tip Port 29	33
Ring Port 30	2	Tip Port 30	34
Ring Port 31	3	Tip Port 31	35
Ring Port 32	4	Tip Port 32	36
Ring Port 33	5	Tip Port 33	37
Ring Port 34	6	Tip Port 34	38
Ring Port 35	7	Tip Port 35	39

Table 19-22 Champ Connector Pin Assignments—Side-A EIA, Connectors J10 and J11; Side-B EIA, Connectors J23 and J24 (continued)

Signal	Pin	Signal	Pin
Ring Port 36	8	Tip Port 36	40
Ring Port 37	9	Tip Port 37	41
Ring Port 38	10	Tip Port 38	42
Ring Port 39	11	Tip Port 39	43
Ring Port 40	12	Tip Port 40	44
Ring Port 41	13	Tip Port 41	45
Ring Port 42	14	Tip Port 42	46
Ring Port 43	15	Tip Port 43	47
Ring Port 44	16	Tip Port 44	48
Ring Port 45	17	Tip Port 45	49
Ring Port 46	18	Tip Port 46	50
Ring Port 47	19	Tip Port 47	51
Ring Port 48	20	Tip Port 48	52
Ring Port 49	21	Tip Port 49	53
Ring Port 50	22	Tip Port 50	54
Ring Port 51	23	Tip Port 51	55
Ring Port 52	24	Tip Port 52	56
Ring Port 53	25	Tip Port 53	57
Ring Port 54	26	Tip Port 54	58
Ring Port 55	27	Tip Port 55	59
Ring Port 56	28	Tip Port 56	60
Unused	29	Unused	61
Unused	30	Unused	62
Unused	31	Unused	63
Unused	32	Unused	64

Note Refer to the “Shelf Assembly Hardware” chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for specific information on DS-1 cables and DS-1 connectors, including product numbers and compatibility.

Step 2 Connect the male connector on the cable to the female connector on the electrical interface assembly (EIA) at the back of the ONS 15310-MA.

Step 3 Tighten the two thumbscrews on the male connector.

Step 4 Return to your originating procedure (NTP).

DLP-C259 Install DS-3/EC-1 Cables

Purpose	This task installs the DS-3/EC-1 cables to connect DS-3/EC-1 signals to the ONS 15310-MA.
Tools/Equipment	Shielded coaxial cable terminated with BNC connectors for DS-3/EC-1 ports BNC insertion/removal tool (see the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for information about obtaining the BNC insertion/removal tool)
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

Step 1 Place the cable connector over the desired connection point on the backplane.

Step 2 Using the BNC insertion tool, position the cable connector so that the slot in the connector is over the corresponding notch at the backplane connection point.

Step 3 Gently push the connector down until the notched backplane connector slides into the slot on the cable connector.

Step 4 Turn the cable connector clockwise to lock it into place.

Step 5 Tie wrap or lace the cables to the EIA according to Telcordia standards (GR-1275-CORE) or local site practice.

Step 6 Return to your originating procedure (NTP).

DLP-C260 Route Cables

Purpose	This task routes electrical, optical, alarm, and timing cables away from the ONS 15310-MA. You can install optional tie-bars specifically designed for the ONS 15310-MA.
Tools/Equipment	Tie-wraps or other securing devices, according to local practice Tie-bar(s)
Prerequisite Procedures	NTP-C158 Install the Electrical Cables, page 2-24 NTP-C160 Install Optical Cables, page 2-28 NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 As needed, install a tie-bar or other strain-relief device, according to local site practice.

⚠ **Caution** You must provide some type of strain relief for the ONS 15310-MA cabling.

Step 2 Route the cables to the appropriate side of the shelf assembly according to local site practice.

Step 3 Secure the cables to the strain-relief device using tie-wraps or other site-specific methods.

Step 4 Label all cables at each end of the connection to avoid confusion with cables that are similar in appearance.

Step 5 Return to your originating procedure (NTP).

DLP-C264 Clear All PM Thresholds

Purpose	This task clears and resets all PM thresholds to default values.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

⚠ **Caution** Pressing the Reset button can mask problems if used incorrectly. This button is commonly used for testing purposes.

Step 1 In node view, double-click the card where you want to view PM thresholds. The card view appears.

Step 2 Click the **Provisioning** > **Thresholds** tab. The subtab names vary depending on the card selected.

Step 3 Click **Reset to Default**.

Step 4 Click **Yes** in the Reset to Default dialog box.

Step 5 Verify that the PM thresholds have been reset.

Step 6 Return to your originating procedure (NTP).

DLP-C265 Set Up a Solaris Workstation for a Craft Connection to an ONS 15310-CL or ONS 15310-MA

Purpose	This task sets up a Solaris workstation for a craft connection to the ONS 15310-CL/ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Log into the workstation as the root user.

Step 2 Check to see if the interface is plumbed by typing:

# **ifconfig** *device*

For example:

# **ifconfig hme1**

If the interface is plumbed, a message similar to the following appears:

```
hme1:flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 2 inet 0.0.0.0 netmask
0
```

If a message similar to this one appears, go to Step 4.

If the interface is not plumbed, a message similar to the following appears:

```
ifconfig: status: SIOCGLIFFLAGS: hme1: no such interface.
```

If a message similar to this one appears, go to Step 3.

Step 3 Plumb the interface by typing:

# ifconfig *device* **plumb**

For example:

# ifconfig hme1 plumb

Step 4 Configure the IP address on the interface by typing:

# ifconfig *interface ip-address* **netmask** *netmask* **up**

For example:

# ifconfig hme0 192.1.0.3 netmask 255.255.255.0 up

Note Enter an IP address that is identical to the ONS 15310-CL/ONS 15310-MA IP address except for the last octet. The last octet must be 1 or 3 through 254.

Step 5 In the Subnet Mask field, type **255.255.255.0**. Skip this step if you checked Enable Socks Proxy on Port and External Network Element (ENE) at Provisioning > Network > General > Gateway Settings.

Step 6 Test the connection:

a. Start Netscape Navigator.

b. Enter the ONS 15310-CL/ONS 15310-MA IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box appear. If this occurs, go to Step 2 of the "DLP-C29 Log into CTC" task on page 17-44 to complete the login. If the Login dialog box does not appear, complete Steps c and d.

c. At the prompt, type:

ping *ONS 15310-CL/ONS 15310-MA-IP-address*

or

For example, to connect to an ONS 15310-CL with a default IP address of 192.1.0.2, type:

ping 192.1.0.2

If your workstation is connected to the ONS 15310-CL/ONS 15310-MA, the following message appears:

IP-address is alive

Note Skip this step if you checked Enable Socks Proxy on Port and External Network Element (ENE) at Provisioning > Network > General > Gateway Settings.

d. If CTC is not responding, a "Request timed out" (Windows) or a "no answer fromx.x.x.x" (UNIX) message appears. Verify the IP and subnet mask information. Check that the cables connecting the workstation to the ONS 15310-CL/ONS 15310-MA are securely attached. Check the link status by typing:

# ndd -set /dev/*device* **instance 0**

# ndd -get /dev/*device* **link_status**

For example:

# ndd -set /dev/hme instance 0

# ndd -get /dev/hme link_status

A result of "1" means the link is up. A result of "0" means the link is down.

Note Check the man page for ndd. For example: **# man ndd**.

Step 7 Return to your originating procedure (NTP).

DLP-C266 Install the CTC Launcher Application from a Release 8.5 Software CD

Purpose	This task installs the CTC Launcher from a Release 8.5 software CD.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Insert the Cisco ONS 15454 or Cisco ONS 15454 SDH or Cisco ONS 15310-CL or Cisco ONS 15310-MA Software Release 8.5 CD into your CD drive.

Step 2 Navigate to the CtcLauncher directory.

Step 3 Save the StartCTC.exe file to a local hard drive.

Step 4 Return to your originating procedure (NTP).

DLP-C267 Install the CTC Launcher Application from a Release 8.5 Node

Purpose	This task installs the CTC Launcher from an ONS 15310-CL or ONS 15310-MA node running Software R8.5.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Using a web browser, go to the following address, where *node-name* is the DNS name of a node you are going to access:

http://*node-name***/fs/StartCTC.exe**

The browser File Download dialog box appears.

Step 2 Click **Save.**

Step 3 Navigate to the location where you want to save the StartCTC.exe file on the local hard drive.

Step 4 Click **Save**.

Step 5 Return to your originating procedure (NTP).

DLP-C268 Connect to ONS Nodes Using the CTC Launcher

Purpose	This task starts the CTC Launcher from an ONS node.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Start the CTC Launcher:

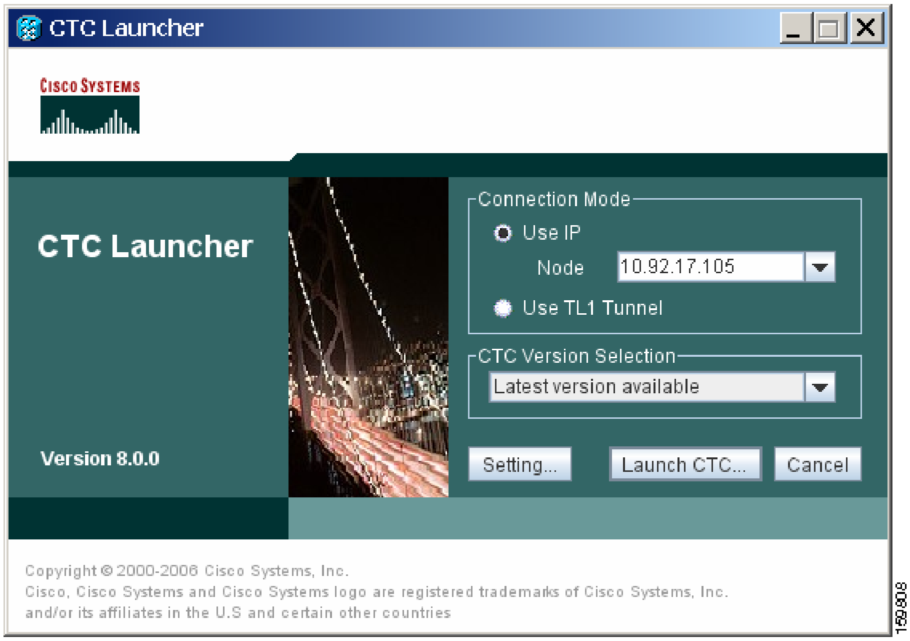
- Windows: navigate to the directory containing the StartCTC.exe file and double-click it. (You can also use the Windows Start menu Run command.)
- Solaris: assuming the StartCTC.exe file is accessible from the current shell path, navigate to the directory containing the CtcLauncher.jar file and type:

  % java -jar StartCTC.exe

Step 2 In the CTC Launcher dialog box, choose **Use IP**.

Figure 19-14 shows the CTC Launcher window.

Figure 19-14 CTC Launcher Window



● Use IP

Node: 10.92.17.105

○ Use TL1 Tunnel

CTC Version Selection: Latest version available

Copyright © 2000-2006 Cisco Systems, Inc.
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.
and/or its affiliates in the U.S and certain other countries

Step 3 In the Login Node box, enter the ONS NE node name or IP address. (If the address was entered previously, you can choose it from the drop-down menu.)

Step 4 Select the CTC version you want to launch from the following choices in the drop-down menu:

- Same version as the login node: Select if you want to launch the same CTC version as the login node version, even if more recent versions of CTC are available in the cache.

- Latest version available: Select if you want to launch the latest CTC version available. If the cache has a newer CTC version than the login node, that CTC version will be used. Otherwise the same CTC version as the login node will be used.
- Version x.xx: Select if you want to launch a specific CTC version.

Note Cisco recommends that you always use the "Same version as the login node" unless the use of newer CTC versions is needed (for example, when CTC must manage a network containing mixed version NEs).

Step 5 Click **Launch CTC**. After the connection is made, the CTC Login dialog box appears.

Step 6 Log into the ONS node.

Note Because each CTC version requires particular JRE versions, the CTC Launcher will prompt the user for the location of a suitable JRE whenever a new CTC version is launched for the first time using a file chooser dialog (if a suitable JRE version is not known by the launcher yet). That JRE information is then saved in the user's preferences file. From the selection dialog, select any appropriate JRE directory.

After the JRE version is selected, the CTC will be launched. The required jar files will be downloaded into the new cache if they are missing. The CTC Login window will appear after a few seconds.

Step 7 Return to your originating procedure (NTP).

DLP-C269 Create a TL1 Tunnel Using the CTC Launcher

Purpose	This task creates a TL1 tunnel using the CTC Launcher, and the tunnel transports the TCP traffic to and from ONS ENEs through the OSI-based GNE.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Double-click the StartCTC.exe file.

Step 2 Click **Use TL1 Tunnel**.

Step 3 In the Open CTC TL1 Tunnel dialog box, enter the following:

- Far End TID—Enter the TID of the ONS ENE at the far end of the tunnel. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.

- Host Name/IP Address—Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS node through an OSI DCC network. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
- Choose a port option:
  - Use Default TL1 Port—Choose this option if you want to use the default TL1 port 3081 and 3082.
  - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient encoding mode. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 4 Click **OK**.

Step 5 If the GNE Login Required box is checked, complete the following steps. If not, continue Step 6.

a. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 6 When the CTC Login dialog box appears, complete the CTC login.

Step 7 Return to your originating procedure (NTP).

DLP-C270 Create a TL1 Tunnel Using CTC

Purpose	This task creates a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click **Create**.

Step 3 In the Create CTC TL1 Tunnel dialog box, enter the following:

- Far End TID—Enter the TID of the ONS ENE at the far end of the tunnel. The ENE must be a Cisco ONS NE. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.
- Host Name/IP Address—Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
- Choose a port option:
  - Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
  - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 4 Click **OK**.

Step 5 If the GNE Login Required box is checked, complete the following steps. If not, continue Step 6.

a. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 6 After the CTC Login dialog box appears, log into CTC.

Step 7 Return to your originating procedure (NTP).

DLP-C271 View TL1 Tunnel Information

Purpose	This task views a TL1 tunnel created using the CTC Launcher.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Log into CTC.

Step 2 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 3 In the TL1 Tunnels window, view the information shown in Table 19-23.

Table 19-23 TL1 Tunnels Window

Item	Description
Far End TID	The Target ID of the NE at the far end of the tunnel. This NE is an ONS NE. It is typically connected with an OSI DCC to a third-party vender GNE. CTC manages this NE.
GNE Host	The GNE host or IP address through which the tunnel is established. This is generally a third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
Port	The TCP port number where the GNE accepts TL1 connections coming from the DCN. These port numbers are standard (such as 3081 and 3082) unless custom port numbers are provisioned on the GNE.
TL1 Encoding	Defines the TL1 encoding used for the tunnel: • LV + Binary Payload— TL1 messages are delimited by an LV (length value) header. TCP traffic is encapsulated in binary form. • LV + Base64 Payload— TL1 messages are delimited by an LV header. TCP traffic is encapsulated using the base 64 encoding. • Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
GNE TID	The GNE TID is shown when the GNE requires a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs. If present, CTC asks the user for the ACT-USER user ID and password when the tunnel is opened.
State	Indicates the tunnel state: OPEN—A tunnel is currently open and carrying TCP traffic. RETRY PENDING—The TL1 connection carrying the tunnel has been disconnected and a retry to reconnect it is pending. (CTC automatically attempts to reconnect the tunnel at regular intervals. During that time all ENEs behind the tunnel are unreachable.) (empty)—No tunnel is currently open.
Far End IP	The IP address of the ONS NE that is at the far end of the TL1 tunnel. This information is retrieved from the NE when the tunnel is established.
Sockets	The number of active TCP sockets that are multiplexed in the tunnel. This information is automatically updated in real time.
Retries	Indicates the number of times CTC tried to reopen a tunnel. If a network problem causes a tunnel to go down, CTC automatically tries to reopen it at regular intervals. This information is automatically updated in real time.
Rx Bytes	Shows the number of bytes of management traffic that were received over the tunnel. This information is automatically updated in real time.
Tx Bytes	Shows the number of bytes of management traffic that were transmitted over the tunnel. This information is automatically updated in real time.

Step 4 Return to your originating procedure (NTP).

DLP-C272 Edit a TL1 Tunnel Using CTC

Purpose	This task edits a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click the tunnel you want to edit.

Step 3 Click **Edit**.

Step 4 In the Edit CTC TL1 Tunnel dialog box, edit the following:

- Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
- Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 5 Click **OK**.

Step 6 If the GNE Login Required box is checked, complete login in the Login to Gateway NE dialog box. If not, continue Step 6.

a. In the UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 7 When the CTC Login dialog box appears, complete the CTC login. Refer to login procedures in the user documentation for the ONS ENE.

Step 8 Return to your originating procedure (NTP).

DLP-C273 Delete a TL1 Tunnel Using CTC

Purpose	This task deletes a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click the tunnel you want to delete.

Step 3 Click **Delete**.

Step 4 In the confirmation dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C274 Provision the Designated SOCKS Servers

Purpose	This task identifies the ONS 15310-CL and ONS 15310-MA SOCKS servers in SOCKS-proxy-enabled networks. Identifying the SOCKS servers reduces the amount of time required to log into a node and have all NEs appear in network view (NE discovery time). The task is recommended when the combined CTC login and NE discovery time is greater than five minutes in networks with SOCKS proxy enabled. Long (or failed) login and NE discovery times can occur in networks that have a high ENE-to-GNE ratio and a low number of ENEs with LAN connectivity.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note To complete this task, you must have either the IP addresses or DNS names of all ONS 15310-CL and ONS 15310-MAs nodes in the network with LAN access that have SOCKS proxy enabled.

Note SOCKS proxy servers can be any accessible ONS network nodes that have LAN access, including the ONS 15310-MA, ONS 15310-CL, ONS 15327, ONS 15454, ONS 15454 SDH, ONS 15600, and ONS 15600 SDH nodes.

Note You must repeat this task any time that changes to SOCKS proxy server nodes occur, for example, whenever LAN connectivity is added to or removed from a node, or when nodes are added or removed from the network.

Note If you cannot log into a network node, complete the "DLP-C29 Log into CTC" task on page 17-44 choosing the Disable Network Discovery option. Complete this task, then login again with network discovery enabled.

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

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

Step 3 In the Designated SOCKS Server field, type the IP address or DNS node name of the first ONS 15310-CL or ONS 15310-MA SOCKS server. The ONS 15310-CL or ONS 15310-MA that you enter must have SOCKS proxy server enabled, and it must have LAN access.

Step 4 Click **Add**. The node is added to the SOCKS server list. If you need to remove a node on the list, click **Remove**.

Step 5 Repeat Steps 3 and 4 to add all qualified ONS 15310-CL or ONS 15310-MA nodes within the network. All ONS nodes that have SOCKS proxy enabled and are connected to the LAN should be added.

Step 6 Click **Check All Servers**. A check is conducted to verify that all nodes can perform as SOCKS servers. If so, a check is placed next to the node IP address or node name in the SOCKS server list. An X placed next to the node indicates one or more of the following:

- The entry does not correspond to a valid DNS name.
- The numeric IP address is invalid.
- The node cannot be reached.
- The node can be reached, but the SOCKS port cannot be accessed, for example, a firewall problem might exist.

Step 7 Click **Apply**. The list of ONS 15310-CL or ONS 15310-MA nodes, including ones that received an X in Step 6, are added as SOCKS servers.

Step 8 Click **OK** to close the Preferences dialog box.

Step 9 Return to your originating procedure (NTP).

DLP-C275 Install or Reinstall the CTC JAR Files

Purpose	This task installs or reinstalls the CTC JAR files into the CTC cache directory on your PC. This is useful when you are using a new CTC version and want to install or reinstall the CTC JAR files without logging into a node or using the StartCTC application (StartCTC.exe).
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Insert the Cisco ONS 15310-CL or Cisco ONS 15310-MA Software Release 8.5 CD into your CD drive.

Step 2 Navigate to the CacheInstall directory.

Note The CTC cache installer is also available on Cisco.com. If you are downloading the SetupCtc-*version*.exe (where *version* is the release version, for example, SetupCtc-085000.exe) file from Cisco.com, skip Step 1 and Step 2.

Step 3 Copy the SetupCtc-*version*.exe file to your local hard drive. Use any location that is convenient for you to access, such as the Windows desktop. Ensure that you have enough disk space to copy and extract the SetupCtc-*version*.exe file.

Step 4 Double-click the SetupCtc-*version*.exe file. This creates a directory named SetupCtc-*version* (at the same location), which contains the LDCACHE.exe file and other CTC files.

Step 5 Double-click the LDCACHE.exe file to install or reinstall the new CTC JAR files into the CTC cache directory on your PC.

Step 6 Return to your originating procedure (NTP).

DLP-C276 Configuring Windows Vista to Support CTC

Purpose	This task describes the configurations that must be done in Windows Vista operating system prior to launching CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Complete the following steps to disable Internet Explorer 7 protected mode:

Note Performa full installation of Windows Vista operating system on your computer. If Windows Vista is installed through operating system upgrade, then CTC will not work. Refer to the manufacturer's user guide for instructions on how to install Windows Vista.

Note If you start CTC by downloading the CTC Launcher application from the node then you do need to perform this procedure. See DLP-C267 Install the CTC Launcher Application from a Release 8.5 Node, page 19-82. This procedure is needed only if CTC is launched from the Internet Explorer browser.

a. Open Internet Explorer,

b. Click **Tools > Internet** Options.

c. Click **Security** tab.

d. Select the zone that is appropriate. Available options are: **Local Intranet** ,**Internet**, and **Trusted Sites**.

e. Check the **Disable Protect Mode** check box.

Step 2 Complete the following steps to Disable TCP Autotuning:

a. From the Windows Start menu, click **Search > Search for Files and Folders.** The Search window appears.

b. On the right side of the window in the Search box, type **Command Prompt** and press **Enter**. Windows will search for the Command Prompt application and list it in the search results.

c. Right click **cmd** and select **Run as administrator**.

d. Enter the administrator user ID and password and click **OK.**

e. A Command prompt windows appears. At the command prompt enter the following text:

```
netsh interface tcp set global autotuninglevel=disabled
```

Autotuning can be enabled if desired using the following command:

```
netsh interface tcp set global autotuninglevel=normal
```

Step 3 Return to your originating procedure (NTP).

DLP-C277 Create User Defined Alarm Types

Purpose	This task creates alarm types for external alarms on the 15310-CL-CTX and CTX2500.
Tools/Equipment	None
Prerequisite Procedures	"DLP-C29 Log into CTC" task on page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The alarms and controls are provisioned using the 15310-CL-CTX and CTX2500 card view. For information about the 15310-CL-CTX and CTX2500 external alarms and controls, virtual wire, and orderwire, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*

Step 1 In the node view, double-click the active 15310-CL-CTX or CTX2500 card. The card view appears.

Step 2 Click the **Provisioning > External Alarms > User Defined Alarms** tabs.

Step 3 Click **Add**. The **Enter New Alarm Type** dialog box will display.

Step 4 In the name field type the new alarm type name and click **OK**.

- The name can be up to 20 alphanumeric characters (upper case). No spaces, no special characters, hyphen (-) is allowed.
- Up to 50 different Alarm Types can be defined.

Step 5 Click the **External Alarms** tab.

Step 6 Verify that the defined name appears in the **Alarm Type** drop-down list.

Step 7 Return to your originating procedure (NTP).

DLP-C278 Configure Link Integrity Timer

Purpose	This task sets the link integrity soak timer for each port in the Ethernet card.
Tools/Equipment	None
Prerequisite Procedures	"DLP-C29 Log into CTC" task on page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click a card to open the card view.

Step 2 In the card view, click the **Provisioning** > **Ether Ports** tabs.

Step 3 In the Line area, enable the link integrity soak timer feature by unchecking the check box in the Link Integrity Disable column for the corresponding port number.

Note If the check box under the Link Integrity Disable column is checked, the Link Integrity Timer field for the corresponding port number will be disabled.

Step 4 Enter the desired link integrity soak duration in the Link Integrity Timer column for the corresponding port number. Enter the link integrity soak duration in the range between 200 ms and 10000 ms, in multiples of 100 ms.

Note The default link integrity timer value is 200 ms.

Step 5 Click **Apply** to set the specified link integrity soak timer.

Step 6 Return to your originating procedure (NTP).

DLP-C289 Enable Node Secure Mode

Purpose	This task enables secure mode on the ONS 15310-MA. When secure mode is enabled, two IPv4 addresses are assigned to the node: one address is assigned to the backplane LAN port and the other is assigned to the CTX2500 RJ-45 TCP/IP (LAN) port.
Tools/Equipment	
Prerequisite Procedures	CTX2500 cards must be installed. NTP-C102 Back Up the Database, page 15-2 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note The IPv4 address assigned to the CTX2500 TCP/IP (LAN) port must reside on a different subnet from the backplane LAN port and the ONS 15310-MA default router. Verify that the new IPv4 address meets this requirement and is compatible with the ONS 15310-MA network IPv4 addresses.

Note The node will reboot after you complete this task, causing a temporary disconnection between the CTC computer and the node.

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

Step 2 Click **Change Mode**.

Step 3 Review the information on the Change Secure Mode wizard page and click **Next**.

Step 4 Enter the IPv4 address and subnet mask for the CTX2500 LAN (TCP/IP) port in the CTX2500 Ethernet Port page, . The IPv4 address cannot reside on the same subnet as the backplane LAN port or the ONS 15310-MA default router.

Step 5 Click **Next**.

Step 6 You can modify the backplane IPv4 address, subnet mask, and default router in the Backplane Ethernet Port page, if needed.

Note Normally, you do not need to modify these fields if no ONS 15310-MA network changes have occurred.

Step 7 Click **Next**.

Step 8 On the SOCKS Proxy Server Settings page, choose one of the following options:

- External Network Element (ENE)—If selected, the CTC computer is only visible to the ONS 15310-MA where the CTC computer is connected. The computer is not visible to the DCC-connected nodes. By default, SOCKS proxy is not enabled for an ENE. If SOCKS proxy is disabled, the NE cannot communicate with other secure mode NEs behind the firewall.
- Gateway Network Element (GNE)—If selected, the CTC computer is visible to other DCC-connected nodes. The node prevents IP traffic from being routed between the DCC and the LAN port. By default, configuring the secure node as a GNE also enables SOCKS proxy for communication with other secure NEs.

Step 9 Click **Finish**.

Within the next 30 to 40 seconds, the CTX2500 cards reboot. CTC switches to network view, and the CTC Alerts dialog box appears. In network view, the node changes to gray and the condition changes to DISCONNECTED.

Step 10 In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish. (This may take several minutes.)

Step 11 After the DISCONNECTED condition clears, complete the following steps to suppress the backplane IP address from display in CTC and the LCD. If you do not want to suppress the backplane IP address display, continue with Step 12.

a. Select the node in node view.

b. Click the **Provisioning > Security > Data Comm** tabs.

c. If you do not want the IPv4 address to appear on the LCD, in the LCD IP Setting field, choose **Suppress Display**.

d. If you do not want the IPv4 address to appear in CTC, check the **Suppress CTC IP Address** check box. This removes the IPv4 address from display in the CTC information area and from the Provisioning > Security > Data Comm tab.

e. Click **Apply**.

Note After you turn on secure mode, the CTX2500 IP (LAN) port address becomes the IPv4 address of the node. The backplane LAN port has a different IPv4 address.

Step 12 Return to your originating procedure (NTP).