CHAPTER 22

DLPs A500 to A599

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

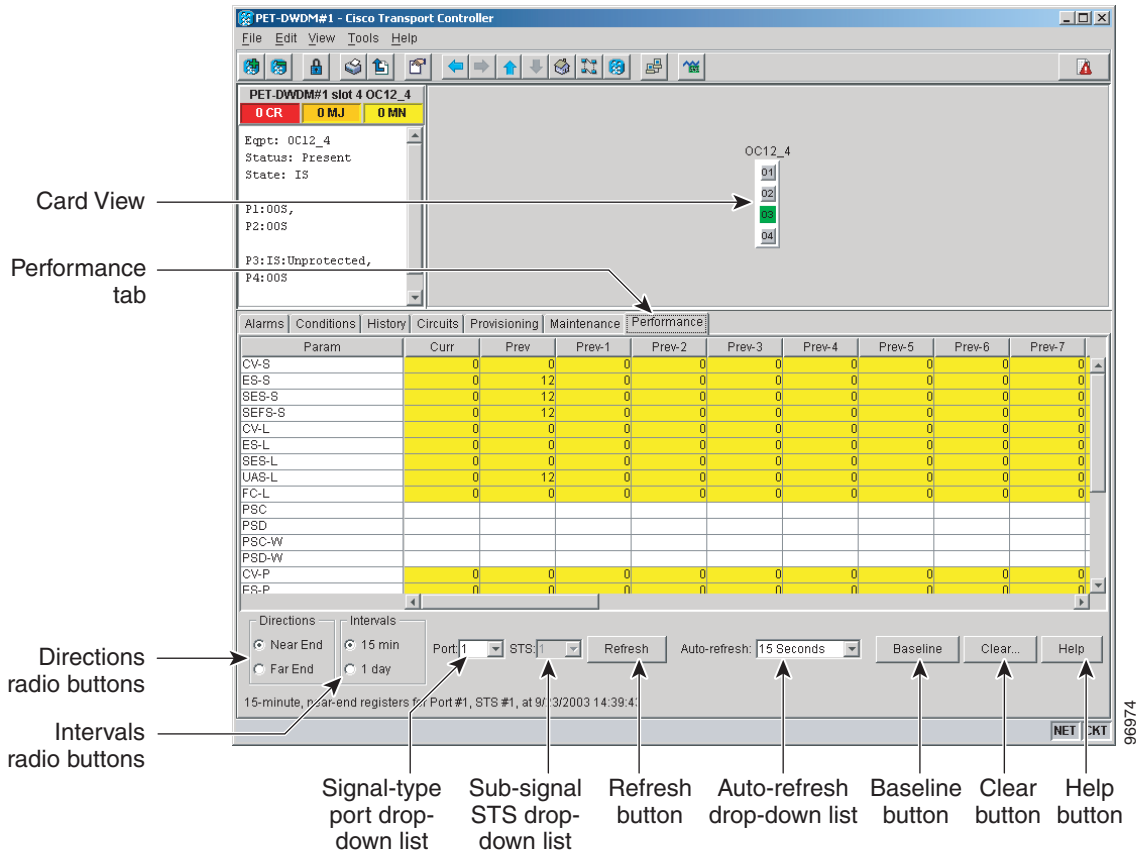
DLP-A507 View OC-N PM Parameters

Purpose	This task enables you to view performance monitoring (PM) counts on an OC-N card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

Step 2 Click the **Performance** tab (Figure 22-1).

Figure 22-1 Viewing OC-N Card Performance Monitoring Information



Step 3 In the Port drop-down list, click the port you want to monitor.

Step 4 Click **Refresh**.

Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current), and Prev-*n* (previous) columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 6 To monitor another port on a multiport card, choose another port from the Port drop-down list and click **Refresh**.

Step 7 Return to your originating procedure (NTP).

DLP-A509 Provision CE-1000-4 Ethernet Ports

Purpose	This task provisions CE-1000-4 Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can provision SONET contiguous concatenated (CCAT) or virtual concatenated (VCAT) circuits for the CE-1000-4 before or after provisioning the card's Ethernet ports and/or packet-over-SONET (POS) ports. See the "NTP-A257 Create an Automatically Routed Optical Circuit" procedure on page 6-38 or the "NTP-A264 Create an Automatically Routed VCAT Circuit" procedure on page 6-82, as needed.

Note CCAT circuits can be created only if a contiguous pool of STSs is available. The Ethernet ports are automatically allocated STSs from the available Cisco ONS 15454 SONET bandwidth on the CE-1000-4 card.

Step 1 In node view, double-click the CE-1000-4 card graphic to open the card.

Step 2 Click the **Provisioning > Ether Ports** tabs.

Step 3 For each CE-1000-4 port, provision the following parameters:

- Port Name— If you want to label the port, enter the port name.

Note Circuit table displays port name of the POS port and not the Ethernet port.

- Admin State— Select the service state for the port. See the "DLP-A214 Change the Service State for a Port" task on page 19-9 for more information.
- Flow Control— Select the flow control for the port. Possible values are **None**, **Symmetrical**, and **Pass Through**.
- Auto Negotiation— Click this check box to enable autonegotiation on the port (default). If you do not want to enable autonegotiation control, uncheck the box.
- MTU— If you want to permit the acceptance of jumbo size Ethernet frames, choose 10004(default). If you do not want to permit jumbo size Ethernet frames, choose 1548.
- Watermark— Select the flow control watermark for the port. To provision the Low Latency flow control watermark, choose **Low Latency** from the drop-down list. The Flow Ctrl Lo and Flow Ctrl Hi values change. To provision a Custom flow control watermark, choose **Custom** from the drop-down list. Enter values in the Flow Ctrl Hi and Flow Ctrl Lo columns. The Flow Ctrl Lo value has a valid range from 1 to 510 and the Flow Ctrl Hi value has a valid range from 2 to 511. The Flow Ctrl Lo value must be lower than the Flow Ctrl Hi value.

Step 4 Click **Apply**.

Step 5 Refresh the Ethernet statistics:

a. Click the **Performance > Ether Ports > Statistics** tabs.

b. Click **Refresh**.

Note Reprovisioning an Ethernet port on the CE-1000-4 card does not reset the Ethernet statistics for that port.

Step 6 Return to your originating procedure (NTP).

DLP-A510 Provision a DS-3 Circuit Source and Destination

Purpose	This task provisions an electrical circuit source and destination for a DS-3 circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

Step 1 From the Node drop-down list, choose the node where the source will originate.

Step 2 From the Slot drop-down list, choose the slot containing the DS-3 card where the circuit will originate. If you are configuring a DS-3 circuit with a transmux card, choose the DS3XM-6 or DS3XM-12 card.

Step 3 From the Port drop-down list, choose the source DS-3, DS3/EC1-48, DS3XM-6, or DS3XM-12 card as appropriate.

Step 4 If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection, click **Use Secondary Source** and repeat Steps 1 through 3 to define the secondary source. If you do not need to create a secondary source, continue with Step 5.

Step 5 Click **Next**.

Step 6 From the Node drop-down list, choose the destination (termination) node.

Step 7 From the Slot drop-down list, choose the slot containing the destination card. The destination is typically a DS3XM-6 or DS-3 card. You can also choose an OC-N card to map the DS-3 circuit to a synchronous transport signal (STS).

Step 8 Depending on the destination card, choose the destination port or STS from the drop-down lists that appear based on the card selected in Step 2. See Table 6-2 on page 6-3 for a list of valid options. Cisco Transport Controller (CTC) does not display ports, STSs, Virtual Tributaries (VTs), or DS3s if they are already in use by other circuits. If you and another user who is working on the same network choose the same port, STS, VT, port, or DS3 simultaneously, one of you receives a Path in Use error and is unable to complete the circuit. The user with the partial circuit needs to choose new destination parameters.

Step 9 If you need to create a secondary destination, for example, a path protection bridge/selector circuit exit point in a multivendor path protection, click **Use Secondary Destination** and repeat Steps 6 through 8 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

DLP-A512 Change Node Access and PM Clearing Privilege

Purpose	This task provisions the physical access points and shell programs used to connect to the ONS 15454 and sets the user security level that can clear node PM data.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Step 2 In the Access area, provision the following:

- LAN access—Choose one of the following options to set the access paths to the node:
  - **No LAN Access**—Allows access to the node only through data communications channel (DCC) connections. Access through the TCC2/TCC2P RJ-45 port and backplane is not permitted.
  - **Front only**—Allows access through the TCC2/TCC2P RJ-45 port. Access through the DCC and the backplane is not permitted.
  - **Backplane only**—Allows access through DCC connections and the backplane. Access through the TCC2/TCC2P RJ-45 port is not allowed.
  - **Front and Backplane**—Allows access through DCC, TCC2/TCC2P RJ-45, and backplane connections.
- Restore Timeout—Sets a time delay for enabling of front and backplane access when DCC connections are lost and "DCC only" is chosen in LAN Access. Front and backplane access is enabled after the restore timeout period has passed. Front and backplane access is disabled as soon as DCC connections are restored.

Step 3 In the Shell Access area, set the shell program used to access the node:

- Access State: Allows you to set the shell program access mode to Disable (disables shell access), Non-Secure, Secure. Secure mode allows access to the node using the Secure Shell (SSH) program. SSH is a terminal-remote host Internet protocol that uses encrypted links.
- Telnet Port: Allows access to the node using the Telnet port. Telnet is the terminal-remote host Internet protocol developed for the Advanced Agency Research Project Network (ARPANET). Port 23 is the default.
- Enable Shell Password: If checked, enables the SSH password. To disable the password, you must uncheck the check box and click Apply. You must type the password in the confirmation dialog box and click OK to disable it.

Step 4 In the TL1 Access area, select the desired level of TL1 access. Disabled completely disables all TL1 access; Non-Secure, Secure allows access using SSH.

Step 5 In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: PROVISIONING or SUPERUSER.

Step 6 Select the Enable Craft Port check box to turn on the shelf controller serial ports.

Step 7 Select the EMS access state from the list. Available states are Non-Secure and Secure (allows access using SSH).

In the TCC CORBA (IIOP/SSLIOP) Listener Port area, choose a listener port option:

- **Default - TCC Fixed**—Uses Port 57790 to connect to ONS 15454s on the same side of the firewall or if no firewall is used (default). This option can be used for access through a firewall if Port 57790 is open.
- **Standard Constant**—Uses Port 683 (IIOP) or Port 684 (SSLIOP), the Common Object Request Broker Architecture (CORBA) default port number.
- **Other Constant**—If the default port is not used, type the Internet Inter-ORB Protocol (IIOP) or SSLIOP port specified by your firewall administrator.

Step 8 In the SNMP Access area, set the Simple Network Management Protocol (SNMP) access state to Non-Secure or Disabled (disables SNMP access).

Step 9 Click **Apply**.

Step 10 Return to your originating procedure (NTP).

DLP-A513 Provision CE-100T-8 Ethernet Ports

Purpose	This task provisions CE-100T-8 Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can provision SONET contiguous concatenated (CCAT) or virtual concatenated (VCAT) circuits for the CE-100T-8 before or after provisioning the card's Ethernet ports and/or packet-over-SONET (POS) ports. See the "NTP-A257 Create an Automatically Routed Optical Circuit" procedure on page 6-38 or the "NTP-A264 Create an Automatically Routed VCAT Circuit" procedure on page 6-82, as needed.

Step 1 In node view, double-click the CE-100T-8 card graphic to open the card.

Step 2 Click the **Provisioning > Ether Ports** tabs.

Step 3 For each CE-100T-8 port, provision the following parameters:

- Port Name—If you want to label the port, enter the port name.

Note Circuit table displays port name of the POS port and not the Ethernet port.

- Admin State—Choose **IS** to put the port in service.
- Expected Speed—Choose the expected speed of the device that is or will be attached to the Ethernet port. If you know the speed, choose **100 Mbps** or **10 Mbps** to match the attached device. If you do not know the speed, choosing **Auto** enables autonegotiation for the speed of the port, and the CE-100T-8 port will attempt to negotiate a mutually acceptable speed with the attached device.
- Expected Duplex—Choose the expected duplex of the device that is or will be attached to the Ethernet port. If you know the duplex, choose **Full** or **Half** to match the attached device. If you do not know the duplex, choosing **Auto** enables autonegotiation for the duplex of the port, and the CE-100T-8 port will attempt to negotiate a mutually acceptable duplex with the attached device.
- Enable Flow Control—Click this check box to enable flow control on the port (default). If you do not want to enable flow control, uncheck the box. The CE-100T-8 attempts to negotiate symmetrical flow control with the attached device.
- 802.1Q VLAN CoS—For a class-of-service (CoS)-tagged frame, the CE-100T-8 can map the eight priorities specified in CoS for either priority or best effort treatment. Any CoS class higher than the class specified in CTC is mapped to priority, which is the treatment geared towards low latency. By default, the CoS is set to 7, which is the highest CoS value. The default results in all traffic being treated as best effort.
- IP ToS—The CE-100T-8 can also map any of the 256 priorities specified in IP type-of-service (ToS) to either priority or best effort treatment. Any ToS class higher than the class specified in CTC is mapped to priority, which is the treatment geared towards low latency. By default, the ToS is set to 255, which is the highest ToS value. This results in all traffic being sent to the best effort queue by default.

Note Untagged traffic is treated as best effort.

Note If traffic is tagged with both CoS and IP ToS, then the CoS value is used, unless the CoS value is 7.

Step 4 Click **Apply**.

Step 5 Refresh the Ethernet statistics:

a. Click the **Performance > Ether Ports > Statistics** tabs.

b. Click **Refresh**.

Note Reprovisioning an Ethernet port on the CE-100T-8 card does not reset the Ethernet statistics for that port.

Step 6 Return to your originating procedure (NTP).

DLP-A514 Provision CE-100T-8 and CE-1000-4 POS Ports

Purpose	This task provisions CE-100T-8 or CE-1000-4 POS ports to carry traffic.
Tools/Equipment	None

Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can provision SONET CCAT or VCAT circuits for the CE-100T-8 or CE-1000-4 before or after provisioning the card's Ethernet ports and/or POS ports. See the "NTP-A257 Create an Automatically Routed Optical Circuit" procedure on page 6-38 or the "NTP-A264 Create an Automatically Routed VCAT Circuit" procedure on page 6-82, as needed.

Step 1 In node view, double-click the CE-100T-8 or CE-1000-4 card graphic to open the card.

Step 2 Click the **Provisioning > POS Ports** tabs.

Step 3 For each CE-100T-8 or CE-1000-4 port, provision the following parameters:

- Port Name—If you want to label the port, enter the port name.

Note Circuit table displays port name of the POS port and not the Ethernet port.

- Admin State—Choose **IS** to put the port in service.
- Framing Type—Choose **GPF-F** POS framing (the default) or **HDLC** POS framing. The framing type needs to match the framing type of the POS device at the end of the SONET circuit.
- Encap CRC—With GFP-F framing, the user can configure a **32-bit** cyclic redundancy check (CRC) (the default) or **none** (no CRC). HDLC framing provides a set 32-bit CRC. The CRC should be set to match the CRC of the POS device on the end of the SONET circuit.

Note For more details about the interoperabilty of Optical Networking System (ONS) Ethernet cards, including information on encapsulation, framing, and CRC, refer to the "POS on ONS Ethernet Cards" chapter of the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Note The CE-100T-8 and CE-1000-4 cards use LEX encapsulation, which is the primary POS encapsulation used in ONS Ethernet cards.

Step 4 Click **Apply**.

Step 5 Refresh the POS statistics:

a. Click the **Performance > POS Ports > Statistics** tabs.

b. Click **Refresh**.

Step 6 Return to your originating procedure (NTP).

DLP-A517 View Alarm or Event History

Purpose	This task is used to view past cleared and uncleared ONS 15454 alarm messages at the card, node, or network level. This task is useful for troubleshooting configuration, traffic, or connectivity issues that are indicated by alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Decide whether you want to view the alarm message history at the node, network, or card level.

Step 2 To view node alarm history:

a. Click the **History > Session** tabs to view the alarms and conditions (events) raised during the current session.

b. Click the **History > Shelf** tabs.

If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.

c. Click **Retrieve** to view all available messages for the History > Shelf tabs.

Note Alarms can be unreported when they are filtered out of the display using the Filter button in either tab. See the "DLP-A225 Enable Alarm Filtering" task on page 19-17 for information.

Tip Double-click an alarm in the alarm table or an event (condition) message in the history table to display the view that corresponds to the alarm message. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.

Step 3 To view network alarm history, from node view:

a. From the View menu choose **Go to Network View**.

b. Click the **History** tab.

Alarms and conditions (events) raised during the current session appear.

Step 4 To view card alarm history from node view:

a. From the View menu choose **Go to Previous View**.

b. Double-click a card on the shelf graphic to open the card-level view.

Note TCC2/TCCP cards and cross-connect (XCVT, XC10G, or XC-VXL-10G) cards do not have a card view.

c. Click the **History > Session** tab to view the alarm messages raised during the current session.

d. Click the **History > Card** tab to retrieve all available alarm messages for the card and click **Retrieve**.

If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.

Note The ONS 15454 can store up to 640 critical alarm messages, 640 major alarm messages, 640 minor alarm messages, and 640 condition messages. When any of these limits is reached, the ONS 15454 discards the oldest events in that category.

Raised and cleared alarm messages (and events, if selected) appear.

Step 5 Return to your originating procedure (NTP).

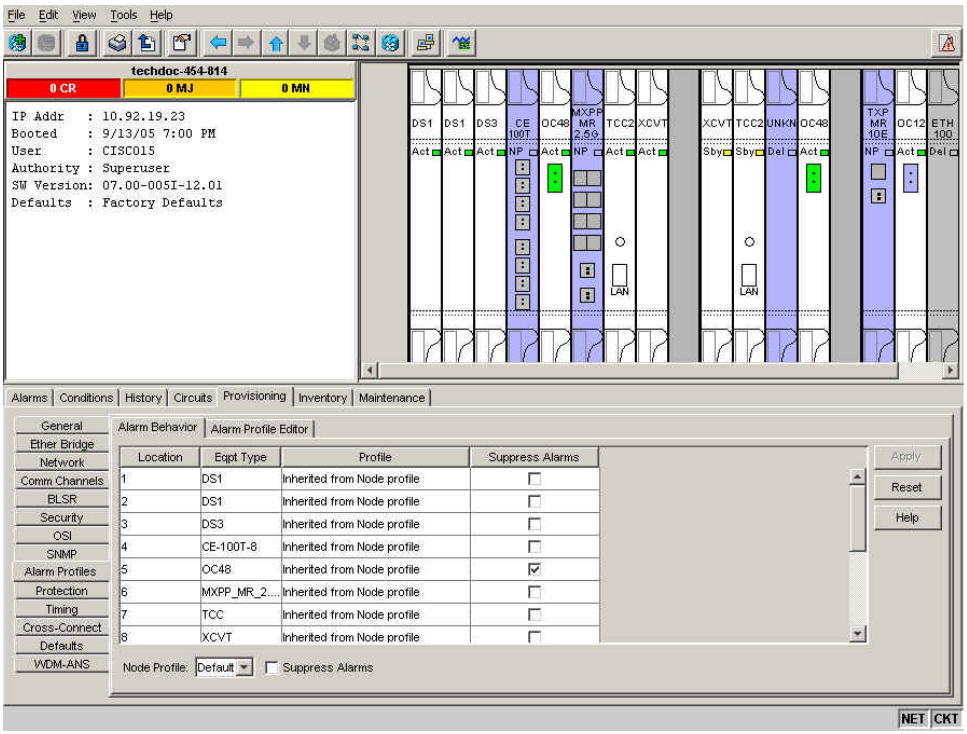
DLP-A518 Create a New or Cloned Alarm Severity Profile

Purpose	This task creates a custom severity profile or clones and modifies the default severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.

Step 2 To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs (Figure 22-2).

Figure 22-2 Node View Alarm Profile Editor



Step 3 To access the profile editor from a card view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 If you want to create a new profile based upon the default profile in use, click **New**. Then go to Step 10.

Step 5 If you want to create a profile using an existing profile located on the node, click **Load** and **From Node** in the Load Profile(s) dialog box.

a. Click the node name you are logged into in the Node Names list.

b. Click the name of an existing profile in the Profile Names list, such as **Default**. Then go to Step 7.

Step 6 If you want to create a profile using an existing profile located in a file that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.

a. Click **Browse**.

b. Navigate to the file location in the **Open** dialog box.

c. Click **Open**.

Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

Step 7 Click **OK**.

The alarm severity profile appears in the Alarm Profiles window. The alarm profile list contains a master list of alarms that is used for a mixed node network. Some of these alarms might not be used in all ONS nodes.

Step 8 Right-click anywhere in the profile column to view the profile editing shortcut menu. (Refer to Step 11 for further information about the Default profile.)

Step 9 Click **Clone** in the shortcut menu.

Tip To see the full list of profiles, including those available for loading or cloning, click Available. You must load a profile before you can clone it.

Step 10 In the New Profile or Clone Profile dialog box, enter a name in the New Profile Name field.

Profile names must be unique. If you try to import or name a profile that has the same name as another profile, CTC adds a suffix to create a new name. Long file names are supported.

Step 11 Click **OK**.

A new alarm profile (named in Step 10) is created. This profile duplicates the default profile severities and appears at the right of the previous profile column in the Alarm Profiles window. You can select it and drag it to a different position.

Note Up to 10 profiles, including the two reserved profiles, Inherited and Default, can be stored in CTC.

The Default profile sets severities to standard Telcordia GR-253-CORE settings. If an alarm has an Inherited profile, it inherits (copies) its severity from the same alarm's severity at the higher level. For example, if you choose the Inherited profile from the network view, the severities at the lower levels (node, card and port) will be copied from this selection. A card with an Inherited alarm profile copies the severities used by the node that contains the card. (If you are creating profiles, you can apply these separately at any level. To do this, complete the "DLP-A117 Apply Alarm Profiles to Cards and Nodes" task on page 18-5.)

Step 12 Modify (customize) the new alarm profile:

a. In the new alarm profile column, click the alarm severity you want to change in the custom profile.

b. Choose a severity from the drop-down list.

c. Repeat Steps a and b for each severity you want to customize. Refer to the following guidelines when you view the alarms or conditions after making modifications:

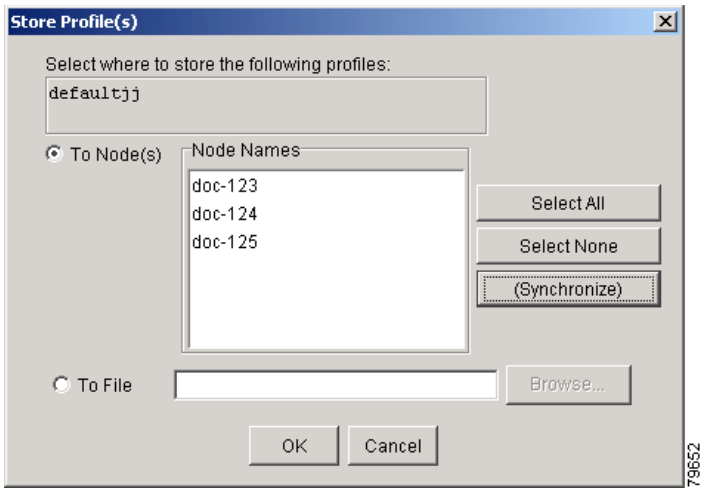
- All Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.
- Default severities are used for all alarms and conditions until you create and apply a new profile.
- Changing a severity to inherited (I) or unset (U) does not change the severity of the alarm.

Step 13 After you have customized the new alarm profile, right-click the profile column to highlight it.

Step 14 Click **Store**.

Step 15 In the Store Profile(s) dialog box, click **To Node(s)** and go to Step a or click **To File** and go to Step b (Figure 22-3).

Figure 22-3 Store Profiles Dialog Box



a. Choose the nodes where you want to save the profile:
   - If you want to save the profile to only one node, click the node in the Node Names list.
   - If you want to save the profile to all nodes, click **Select All**.
   - If you do not want to save the profile to any nodes, click **Select None**.
   - If you want to update alarm profile information, click **(Synchronize)**.

b. Save the profile:
   - Click **Browse** and navigate to the profile save location.
   - Enter a name in the File name field.
   - Click **Select** to choose this name and location. Long file names are supported. CTC supplies a suffix of *.pfl to stored files.
   - Click **OK** to store the profile.

Step 16 As needed, perform any of the following actions:

- Click the **Hide Identical Rows** check box to configure the Alarm Profiles window to view rows with dissimilar severities.
- Click the **Hide Reference Values** check box to configure the Alarm Profiles window to view severities that do not match the Default profile.
- Click the **Only show service-affecting severities** check box to configure the Alarm Profiles window not to display Minor and some Major alarms that will not affect service.

Step 17 Return to your originating procedure (NTP).

DLP-A519 Apply Alarm Profiles to Ports

Purpose	This task applies a custom or default alarm severity profile to a port or ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A518 Create a New or Cloned Alarm Severity Profile, page 22-10 DLP-A60 Log into CTC, page 17-67
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.

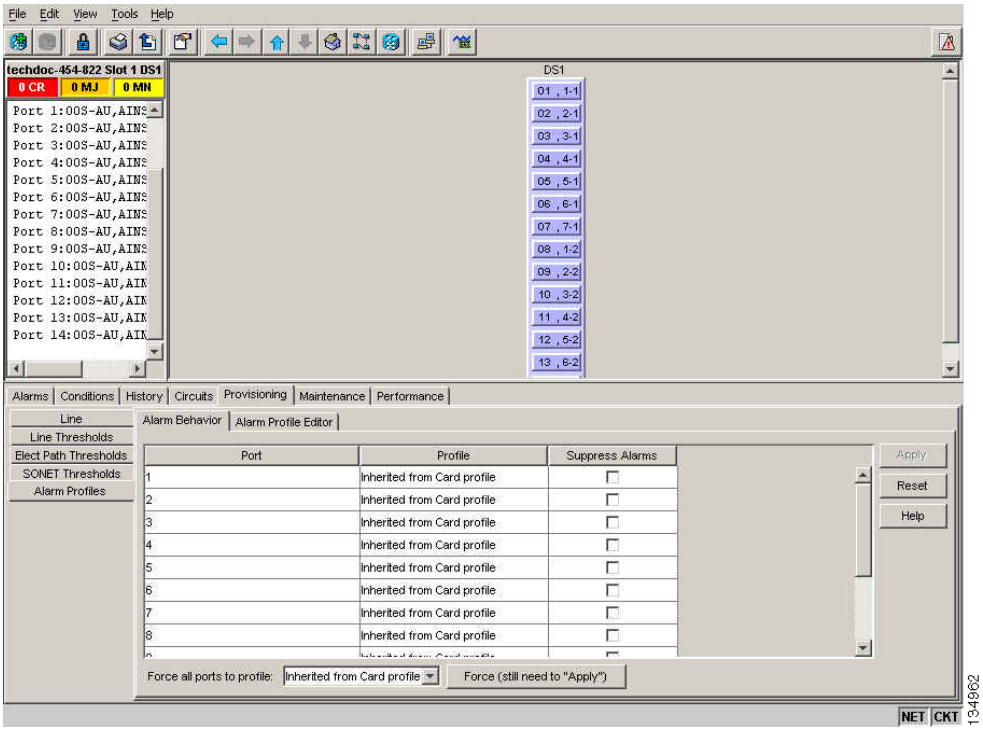
Note You can also apply alarm profiles to cards using the "DLP-A117 Apply Alarm Profiles to Cards and Nodes" task on page 18-5.

Note The card view is not available for the TCC2/TCCP or cross-connect cards.

Step 2 Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Figure 22-4 shows the alarm profiles of DS1/E1-56 card ports. CTC shows Parent Card Profile: Inherited.

Figure 22-4 DS1-N-14 Card Alarm Behavior Tab



Go to Step 3 to apply profiles to a port. Go to Step 4 to apply profiles to all ports on a card.

Step 3 To apply profiles on a port basis:

a. In card view, click the port row in the Profile column.

b. Choose the new profile from the drop-down list.

c. Click **Apply**.

Step 4 To apply profiles to all ports on a card:

a. In card view, click the **Force all ports to profile** drop-down arrow at the bottom of the window.

b. Choose the new profile from the drop-down list.

c. Click **Force (still need to "Apply")**.

d. Click **Apply**.

In node view the Port Level Profiles column indicates port-level profiles with a notation such as "exist (1)" (Figure 18-3 on page 18-6).

Step 5 To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

Step 6 Return to your originating procedure (NTP).

DLP-A520 Delete Alarm Severity Profiles

Purpose	This task deletes a custom or default alarm severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To access the alarm profile editor from network view, go to network view and click the **Provisioning > Alarm Profiles** tabs.

Step 2 To access the profile editor from node view, go to node view and click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

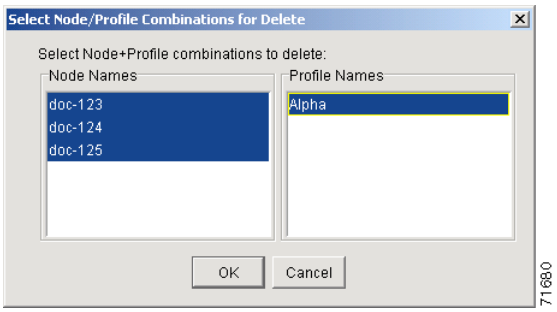
Step 3 To access the profile editor from a card view, double-click the card to display the card view and click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 Click the profile you are deleting to select it.

Step 5 Click **Delete**.

The Select Node/Profile Combination for Delete dialog box appears (Figure 22-5).

Figure 22-5 Select Node/Profile Combination For Delete Dialog Box



Note You cannot delete the Inherited or Default alarm profiles.

Note A previously created alarm profile cannot be deleted unless it has been stored on the node. If the profile is visible on the Alarm Profiles tab but is not listed in the Select Node/Profile Combinations to Delete dialog box, continue with Step 9.

Step 6 Click the node names in the Node Names list to highlight the profile location.

Tip If you hold the Shift key down, you can select consecutive node names. If you hold the Ctrl key down, you can select any combination of nodes.

Step 7 Click the profile names you want to delete in the Profile Names list.

Step 8 Click **OK**.

Click **Yes** in the Delete Alarm Profile dialog box.

Note If you delete a profile from a node, it still appears in the network view Provisioning > Alarm Profile Editor window unless you remove it using the following step.

Step 9 To remove the alarm profile from the window, right-click the column of the profile you deleted and choose **Remove** from the shortcut menu.

Note If a node and profile combination is selected but does not exist, a warning appears: “One or more of the profile(s) selected do not exist on one or more of the node(s) selected.” For example, if node A has only profile 1 stored and the user tries to delete both profile 1 and profile 2 from node A, this warning appears. However, the operation still removes profile 1 from node A.

Note The Default and Inherited special profiles cannot be deleted and do not appear in the Select Node/Profile Combination for Delete Window.

Step 10 Return to your originating procedure (NTP).

DLP-A521 Modify Alarm, Condition, and History Filtering Parameters

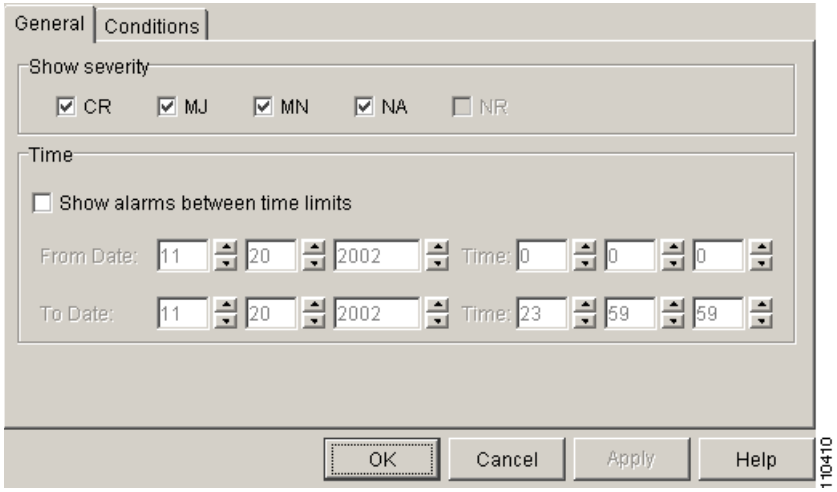
Purpose	This task changes alarm and condition reporting in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A225 Enable Alarm Filtering, page 19-17 DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 At the node, network, or card view, click the **Alarms** tab, **Conditions** tab, or **History** tab.

Step 2 Click the **Filter** button at the lower-left of the bottom toolbar.

The filter dialog box appears, displaying the General tab. Figure 22-6 shows the Alarm Filter dialog box; the Conditions and History tabs have similar dialog boxes.

Figure 22-6 Alarm Filter Dialog Box General Tab



In the General tab Show Severity box, you can choose which alarm severities will show through the alarm filter and provision a time period during which filtered alarms show through the filter. To change the alarm severities shown in the filter, go to Step 3. To change the time period filter for the alarms go to Step 4.

Step 3 In the Show Severity area, click the check boxes for the severities [Critical (CR), Major (MJ), Minor (MN), or Not-Alarmed (NA)] you want to be reported at the network level. Leave severity check boxes deselected (unchecked) to prevent those severities from appearing.

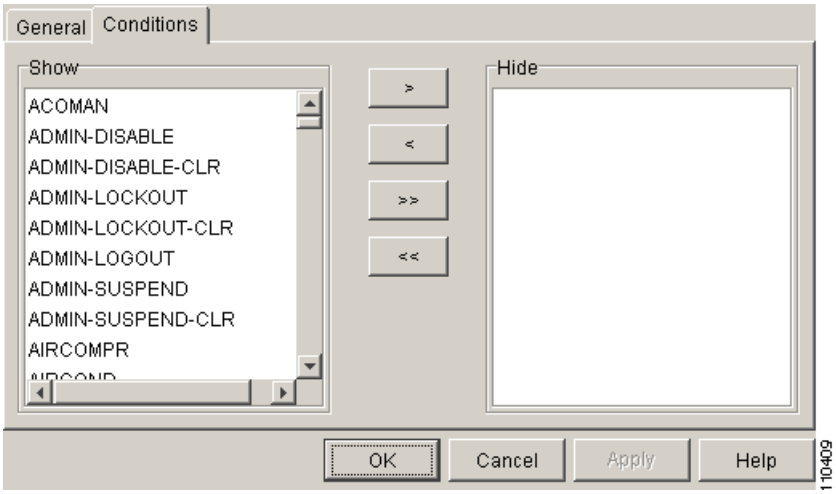
When alarm filtering is disabled, all alarms show.

Step 4 In the Time area, click the **Show alarms between time limits** check box to enable it. Click the up and down arrows in the From Date, To Date, and Time fields to modify what period of alarms are shown.

To modify filter parameters for conditions, continue with Step 5. If you do not need to modify them, continue with Step 6.

Step 5 Click the filter dialog box **Conditions** tab (Figure 22-7).

Figure 22-7 Alarm Filter Dialog Box Conditions Tab



When filtering is enabled, conditions in the Show list are visible and conditions in the Hide list are invisible.

- To move conditions individually from the Show list to the Hide list, click the > button.
- To move conditions individually from the Hide list to the Show list, click the < button.
- To move conditions collectively from the Show list to the Hide list, click the >> button.
- To move conditions collectively from the Hide list to the Show list, click the << button.

Note Conditions include alarms.

Step 6 Click **Apply** and **OK**.

Alarm and condition filtering parameters are enforced when alarm filtering is enabled (see the "DLP-A225 Enable Alarm Filtering" task on page 19-17), and the parameters are not enforced when alarm filtering is disabled (see the "DLP-A227 Disable Alarm Filtering" task on page 19-17).

Step 7 Return to your originating procedure (NTP).

DLP-A522 Suppress Alarm Reporting

Purpose	This task suppresses the reporting of ONS 15454 alarms at the node, card, or port level.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If multiple CTC/TL1 sessions are open, suppressing alarms in one session suppresses the alarms in all other open sessions.

Note Alarm suppression at the node level does not supersede alarm suppression at the card or port level. Suppression can exist independently for all three entities, and each entity will raise separate alarms suppressed by the user command (AS-CMD) alarm.

Step 1 If you are in node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 2 To suppress alarms for the entire node:

a. Check the **Suppress Alarms** check box.

b. Click **Apply**.

All raised alarms for the node will change color to white in the Alarms window and their status will change to cleared. After suppressing alarms, clicking **Synchronize** in the Alarms window will remove cleared alarms from the window. However, an AS-CMD alarm will show in node or card view to indicate that node-level alarms were suppressed, and the word System will appear in the Object column.

Note The only way to suppress BITS, power source, or system alarms is to suppress alarms for the entire node. These cannot be suppressed separately, but the shelf backplane can be.

Step 3 To suppress alarms for individual cards:

a. Locate the card row (using the Location column for the slot number or the Eqpt Type column for the equipment name).

b. Check the **Suppress Alarms column** check box on that row.

Alarms that directly apply to this card will change appearance as described in Step 2. For example, if you suppressed raised alarms for an OC-48 card in Slot 16, raised alarms for this card will change in node or card view. The AS-CMD alarm will show the slot number in the Object number. For example, if you suppressed alarms for a Slot 16 OC-48 card, the AS-CMD object will be “SLOT-16.”

Click **Apply**.

Step 4 To suppress alarms for individual card ports, double-click the card in node view.

Step 5 Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 6 Check the **Suppress Alarms** column check box for the port row where you want to suppress alarms (Figure 22-4 on page 22-14).

Step 7 Click **Apply**.

Alarms that apply directly to this port will change appearance as described in Step 2. (However, alarms raised on the entire card will remain raised.) A raised AS-CMD alarm that shows the port as its object will appear in either alarm window. For example, if you suppressed alarms for Port 1 on the Slot 16 OC-48 card, the alarm object will show "FAC-16-1."

Step 8 Return to your originating procedure (NTP).

DLP-A523 Discontinue Alarm Suppression

Purpose	This task discontinues alarm suppression and reenables alarm reporting on a port, card, or node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A522 Suppress Alarm Reporting, page 22-19 DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If multiple CTC sessions are open, discontinuing suppression in one session will discontinue suppression in all other open sessions.

Step 1 To discontinue alarm suppression for the entire node:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tab.

b. Uncheck the **Suppress Alarms** check box.

Suppressed alarms will reappear in the Alarms window. (They might have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the System object will be cleared in all views.

Step 2 To discontinue alarm suppression for individual cards:

a. In the node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

b. Locate the card that was suppressed in the slot list.

c. Uncheck the Suppress Alarms column check box for that slot.

d. Click **Apply**.

Suppressed alarms will reappear in the Alarms window. (They might have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the slot object (for example, SLOT-16) will be cleared in all views.

Step 3 To discontinue alarm suppression for ports, double-click the card to open the card view and click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 4 Uncheck the **Suppress Alarms** check box for the port(s) you no longer want to suppress.

Step 5 Click **Apply**.

Suppressed alarms will reappear in the Alarms window. (They might have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the port object (for example, FAC-16-1) will be cleared in all views.

Step 6 Return to your originating procedure (NTP).

DLP-A524 Download an Alarm Severity Profile

Purpose	This task downloads a custom alarm severity profile from a network-drive accessible CD-ROM, floppy disk, or hard disk location.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.

Step 2 To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 3 To access the profile editor from a card view, double-click the card to open the card view and click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 Click **Load**.

Step 5 If you want to download a profile that exists on the node, click **From Node** in the Load Profile(s) dialog box.

a. Click the node name you are logged into in the Node Names list.

b. Click the name of the profile in the Profile Names list, such as **Default**.

Step 6 If you want to download a profile that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.

a. Click **Browse**.

b. Navigate to the file location in the **Open** dialog box.

c. Click **Open**.

Note The Default alarm profile list contains alarm and condition severities that correspond when applicable to default values established in Telcordia GR-253-CORE.

Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

Step 7 Click **OK**.

The downloaded profile appears at the right side of the Alarm Profiles window.

Step 8 Right-click anywhere in the downloaded profile column to view the profile editing shortcut menu.

Step 9 Click **Store**.

Step 10 In the Store Profile(s) dialog box, click **To Node(s)**.

a. Choose the nodes where you want to save the profile:
   - If you want to save the profile to only one node, click the node in the Node Names list.
   - If you want to save the profile to all nodes, click **Select All**.
   - If you do not want to save the profile to any nodes, click **Select None**.
   - If you want to update alarm profile information, click (**Synchronize**).

b. **Click OK**.

Step 11 Return to your originating procedure (NTP).

DLP-A526 Change Line and Threshold Settings for the DS3i-N-12 Cards

Purpose	This task changes the line and threshold settings for the DS3i-N-12 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the DS3i-N-12 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

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

Note See Chapter 8, "Manage Alarms" for information about the Alarm Profiles tab.

Note If you want to modify a threshold setting, it might be necessary to click on 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 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 3 through 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 22-1. For definitions of the line threshold settings, see Table 22-2 on page 22-25. For definitions of the electrical path threshold settings, see Table 22-3 on page 22-25. For definitions of the SONET threshold settings, see Table 22-4 on page 22-25.

Table 22-1 describes the values on the Provisioning > Line tabs for the DS3i-N-12 cards.

Table 22-1 Line Options for the DS3i-N-12 Cards

Parameter	Description	Options
Port	(Display only) Port number.	1 to 12
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• Unframed • M13 • C Bit • Auto Provisioned
Detected Line Type	Displays the detected line type.	• M13 • C Bit • Unframed • Unknown
Line Coding	(Display only) Defines the DS3E transmission coding type.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450

Table 22-1 Line Options for the DS3i-N-12 Cards (continued)

Parameter	Description	Options
Admin State	Sets the port administrative 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.
Service State	(Display only) 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—(In-Service and Normal) The port is fully operational and performing as provisioned. • OOS-AU,AINS—(Out-Of-Service and Autonomous, Automatic In-Service) 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—(Out-of-Service and Management, Disabled) The port is out-of-service and unable to carry traffic. • OOS-MA,MT—(Out-of-Service and Management, Maintenance) The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

Table 22-2 describes the parameters on the Provisioning > Line Thresholds tabs for the DS3i-N-12 cards.

Table 22-2 Line Threshold Options for the DS3i-N-12 Cards

Parameter	Description
Port	(Display only) Port number; 1 to 12
CV	Coding violations.
ES	Errored seconds
SES	Severely errored seconds
LOSS	Loss of signal seconds; number of one-second intervals containing one or more LOS defects
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 22-3 describes the parameters on the Provisioning > Elect Path Thresholds tabs for the DS3i-N-12 cards.

Table 22-3 Electrical Path Options for the DS3i-N-12 Cards

Parameter	Description
Port	(Display only) Port number; Port 1 to 12.
CVP	Coding violations - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
ESP	Errored seconds - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
SESP	Severely errored seconds - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
SASP	Severely errored frame/alarm indication signal - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
UASP	Unavailable seconds - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
AISSP	Alarm indication signal seconds - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 22-4 describes the values on the Provisioning > SONET Thresholds tabs for the DS3i-N-12 cards.

Table 22-4 SONET Threshold Options for DS3i-N-12 Cards

Parameter	Description
Port	(Display only) Port number; 1 to 12
CV	Coding violations

Table 22-4 SONET Threshold Options for DS3i-N-12 Cards (continued)

Parameter	Description
ES	Errored seconds
FC	Failure count
SES	Severely errored seconds
UAS	Unavailable seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A527 Change the OC-N Card ALS Maintenance Settings

Purpose	This task changes the automatic laser shutdown (ALS) maintenance settings for the OC-N cards. This feature is available for OC3-8, OC-192, and MRC-12 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the OC-N card where you want to change the ALS maintenance settings.

Step 2 Click the **Maintenance > ALS** tabs.

Step 3 Modify any of the settings described in Table 22-5 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box. The provisionable parameters are listed in the options column in the table.

Step 4 Click **Apply**. If the change affects traffic, a warning message displays. Click **Yes** to complete the change.

Table 22-5 OC-N Maintenance Settings

Parameter	Description	Options
Port number	(Display only) Port number	—
ALS Mode	Automatic laser shutdown mode. ALS provides the ability to shut down the TX laser when the RX detects a loss of signal (LOS).	From the drop-down list, choose one of the following: • Disable—Deactivates ALS. • Auto Restart—(Default) ALS is active. The power is automatically shut down when needed and automatically tries to restart using a probe pulse until the cause of the failure is repaired. • Manual Restart—failure is repaired. • Manual Restart—ALS is active. When conditions that caused the outage are resolved the laser must be manually restarted only if both ends are provisioned in Manual Restart mode . • Manual Restart for Test—Manually restarts the laser for testing.
Recovery Pulse Duration	Sets the recovery laser pulse duration, in seconds, for the initial, recovery optical power pulse following a laser shutdown.	Numeric. For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.
Recovery Pulse Interval	Sets the recovery laser pulse interval, in seconds. This is the period of time that must past before the recover pulse is repeated.	Numeric. For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.
Currently Shutdown	(Display only) Displays the current status of the laser.	Numeric. For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.
Request Laser Restart	If checked, allows you to restart the laser for maintenance. **Note** Restarting a laser might be traffic-affecting.	Checked or unchecked

Step 5 Return to your originating procedure (NTP).

DLP-A528 Change the Default Network View Background Map

Purpose	This task changes the default map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-67
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note If you modify the background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the Edit menu, choose **Preferences > Map** and check the **Use Default Map** check box.

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

Step 3 In the Defaults Selector area, choose **CTC** and then **network**.

Step 4 Click the **Default Value** field and choose a default map from the drop-down list. Map choices are: Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).

Step 5 Click **Apply**. The new network map appears.

Step 6 Click **OK**.

Step 7 If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the ONS 15454 icons are visible. (You can also choose **Fit Graph to Window**.)

Step 8 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 9 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-A529 Delete Ethernet RMON Alarm Thresholds

Purpose	This task deletes remote monitoring (RMON) threshold crossing alarms for Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A533 Create Ethernet RMON Alarm Thresholds, page 22-34 DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15454 ML-Series cards use the Cisco IOS command line interface (CLI) to manage RMON.

Step 1 Double-click the Ethernet card where you want to delete the RMON alarm thresholds.

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

Note For the CE-Series, click the **Provisioning > Ether Ports > RMON Thresholds** tabs or **Provisioning > POS Ports > RMON Thresholds** tabs.

Step 3 Click the RMON alarm threshold you want to delete.

Step 4 Click **Delete**. The Delete Threshold dialog box appears.

Step 5 Click **Yes** to delete the threshold.

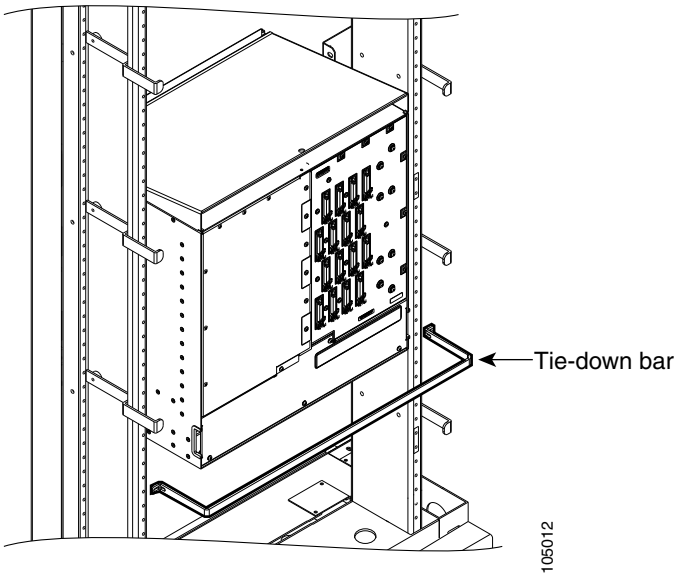
Step 6 Return to your originating procedure (NTP).

DLP-A530 Install the Tie-Down Bar

Purpose	This task installs the tie-down bar used to secure cabling on the rear of the ONS 15454. The tie-down bar can be used to provide a diverse path for redundant power feeds and cables.
Tools/Equipment	Tie-down bar Screws (4)
Prerequisite Procedures	DLP-A5 Mount the Shelf Assembly in a Rack (One Person), page 17-5 DLP-A6 Mount the Shelf Assembly in a Rack (Two People), page 17-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Align the ends of the tie-down bar with the four screw holes located 1 RU below the ONS 15454. Figure 22-8 shows the tie-down bar, the ONS 15454, and the rack.

Figure 22-8 Tie-Down Bar



Step 2 Install the four screws into the rack.

Step 3 Return to your originating procedure (NTP).

DLP-A531 Print CTC Data

Purpose	This task prints CTC card, node, or network data in graphical or tabular format on a Windows-provisioned printer.
Tools/Equipment	Printer connected to the CTC computer by a direct or network connection
Prerequisite procedures	DLP-A60 Log into CTC, page 17-67
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the 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, and card view windows.

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

Step 3 In the Print dialog box, click a printing option (Figure 22-9).

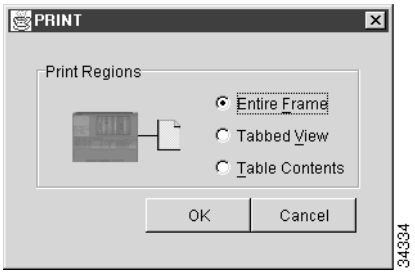
- Entire Frame—Prints the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.

- 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. This option does not apply to the following windows:
  - Provisioning > General tab (General, Power Monitor, and Multishelf Config) windows
  - Provisioning > Network > General windows
  - Provisioning > Security > Policy, Access, and Legal Disclaimer windows
  - Provisioning > SNMP window
  - Provisioning > Timing > General and BITS Facilities windows
  - Provisioning > Cross-Connect window
  - Provisioning > OSI > Main Setup, TARP windows
  - Provisioning > WDM-ANS > Node Setup window
  - Maintenance > Cross-Connect > Cards window
  - Maintenance > Database window
  - Maintenance > Diagnostic window
  - Maintenance > Protection window
  - Maintenance > Timing > Source window

  The Table Contents option prints all the data contained in a table and the table 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 distinguish whether the printout applies to the network, node, or card view. To determine the view, compare the tabs on the printout. The network, node, and card views are identical except that network view does not contain an Inventory tab or Performance tab.

Figure 22-9 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-A532 Export CTC Data

Purpose	This task exports CTC table data as delineated text to view or edit the data in text editor, word processor, spreadsheet, database management, or web browser applications. You can also export data from the Edit Circuits window.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-67
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the 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.

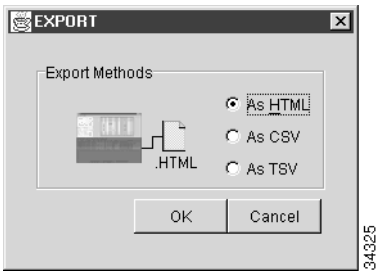
b. In the Edit Circuits window, choose the desired tab: Drops, UPSR Selectors, UPSR Switch Counts, State, or Merge. (Depending on your configuration, you may or may not see all of these tabs.)

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

Step 4 In the Export dialog box, click a data format (Figure 22-10):

- **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 window.
- **As TSV**—Saves the CTC table as tab-separated values (TSV).

Figure 22-10 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 view the CTC data, or you can double-click the file name and choose an application such as Notepad.

Text editor and word processor applications format 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 format 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 does not apply to the following tabular (Save as TSV) data:

- Circuits (Edit option, General and Monitor windows)
- Provisioning > General > General, Power Monitor, and Multishelf Config windows
- Provisioning > Network > General windows
- Provisioning > Security > Policy, Access, and Legal Disclaimer windows
- Provisioning > SNMP window
- Provisioning > Timing > General and BITS FAcilities windows
- Provisioning > OSI > Main Setup window and OSI > TARP > Config window
- Provisioning > Cross-Connect window
- Provisioning > WDM-ANS > Node Setup window
- Maintenance > Cross-Connect > Cards window
- Maintenance > Database window
- Maintenance > Diagnostic window
- Maintenance > Protection window
- Maintenance > Timing > Source windows
- Maintenance > DWDM > ROADM Power Monitoring window

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 a 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-A533 Create Ethernet RMON Alarm Thresholds

Purpose	This procedure sets up remote monitoring (RMON) to allow network management systems to monitor Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15454 ML-Series cards use the Cisco IOS CLI to manage RMON.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-67 at the node where you want to set up RMON. If you are already logged in, continue with Step 2.

Step 2 Double-click the Ethernet card where you want to create the RMON alarm thresholds.

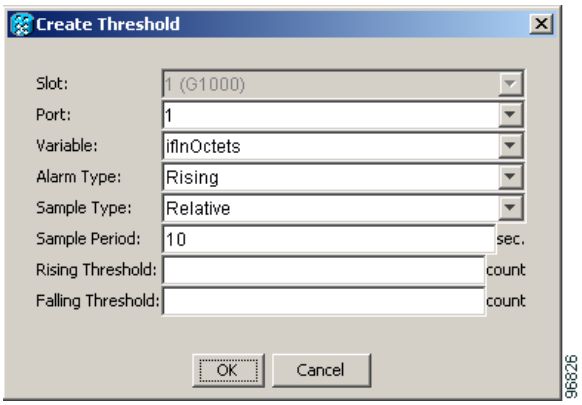
Step 3 In card view, click the **Provisioning > RMON Thresholds** tabs.

Note For CE- and ML-Series Ethernet cards, click the **Provisioning > Ether Ports > RMON Thresholds** tabs or **Provisioning > POS Ports > RMON Thresholds** tabs.

Step 4 Click **Create**.

The Create Ether Threshold dialog box appears (Figure 22-11).

Figure 22-11 Creating RMON Thresholds



Step 5 From the Port drop-down list, choose the applicable port on the Ethernet card you selected.

Step 6 From the Variable drop-down list, choose the variable. See Table 22-6 and Table 22-7 for a list of the Ethernet and POS threshold variables available in this field.

Table 22-6 Ethernet Threshold Variables (MIBs)

Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets
iflnUcastPkts	Total number of unicast packets delivered to an appropriate protocol
ifInMulticastPkts	(G-Series, CE-Series, and ML-Series only) Number of multicast frames received error free
ifInBroadcastPkts	(G-Series, CE-Series, and ML-Series only) The number of packets, delivered by this sublayer to a higher (sub)layer, that were addressed to a broadcast address at this sublayer
ifInDiscards	(G-Series, CE-Series, and ML-Series only) The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol
iflnErrors	Number of inbound packets discarded because they contain errors
ifOutOctets	Total number of transmitted octets, including framing packets
ifOutUcastPkts	Total number of unicast packets requested to transmit to a single address
ifOutMulticastPkts	(G-Series, CE-Series, and ML-Series only) Number of multicast frames transmitted error free
ifOutBroadcastPkts	(G-Series, CE-Series, and ML-Series only) The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent
ifOutDiscards	(G-Series only) The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted
dot3statsAlignmentErrors	Number of frames with an alignment error, that is, the length is not an integral number of octets and the frame cannot pass the frame check sequence (FCS) test
dot3StatsFCSErrors	Number of frames with framecheck errors, that is, there is an integral number of octets, but an incorrect FCS
dot3StatsSingleCollisionFrames	(Not supported by E-Series or G-Series) Number of successfully transmitted frames that had exactly one collision
dot3StatsMutlipleCollisionFrames	(Not supported by E-Series or G-Series) Number of successfully transmitted frames that had multiple collisions
dot3StatsDeferredTransmissions	(Not supported by E-Series or G-Series) Number of times the first transmission was delayed because the medium was busy
dot3StatsLateCollisions	(Not supported by E-Series or G-Series) Number of times that a collision was detected later than 64 octets into the transmission (also added into collision count)

Table 22-6 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
dot3StatsExcessiveCollisions	(Not supported by E-Series or G-Series) Number of frames where transmissions failed because of excessive collisions
dot3StatsCarrierSenseErrors	(G-Series only) The number of transmission errors on a particular interface that are not otherwise counted
dot3StatsSQETestErrors	(G-Series only) A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address; this does not include multicast packets
etherStatsCollisions	An estimate of the total number of collisions on this Ethernet segment. The value returned depends on the location of the RMON probe. Section 8.2.1.3 (10Base5) and Section 10.3.1.3 (10Base2) of the IEEE 802.3 standard state that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus, a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment. Probe location plays a much smaller role when considering 10BaseT. Section 14.2.1.4 (10BaseT) of the IEEE 802.3 standard defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BaseT station can only detect collisions when it is transmitting. Thus, probes placed on a station and a repeater should report the same number of collisions. An RMON probe inside a repeater should report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.

Table 22-6 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
etherStatsCollisionFrames	An estimate of the total number of collisions on this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10Base5) and Section 10.3.1.3 (10Base2) of the IEEE 802.3 standard state that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus, a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment. Probe location plays a much smaller role when considering 10BaseT. Section 14.2.1.4 (10BASE-T) of the IEEE 802.3 standard defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BaseT station can only detect collisions when it is transmitting. Thus, probes placed on a station and a repeater, should report the same number of collisions. An RMON probe inside a repeater should report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.
etherStatsDropEvents	The total number of events in which packets were dropped by the probe due to lack of resources. This number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
etherStatsJabbers	Total number of octets of data (including bad packets) received on the network
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
etherStatsUndersizePkts	Number of packets received with a length less than 64 octets
etherStatsFragments	Total number of packets that are not an integral number of octets or have a bad FCS, and that are less than 64 octets long
etherStatsPkts64Octets	Total number of packets received (including error packets) that were 64 octets in length
etherStatsPkts65to127Octets	Total number of packets received (including error packets) that were 65 to 172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 to 255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 to 511 octets in length

Table 22-6 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 to 1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 to 1518 octets in length
etherStatsJabbers	Total number of packets longer than 1518 octets that were not an integral number of octets or had a bad FCS
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets
etherStatsCollisions	Best estimate of the total number of collisions on this segment
etherStatsCollisionFrames	Best estimate of the total number of frame collisions on this segment
etherStatsCRCAlignErrors	Total number of packets with a length between 64 and 1518 octets, inclusive, that had a bad FCS or were not an integral number of octets in length
receivePauseFrames	(G-Series only) The number of received IEEE 802.x pause frames
transmitPauseFrames	(G-Series only) The number of transmitted IEEE 802.x pause frames
receivePktsDroppedInternalCongestion	(G-Series only) The number of received framed dropped due to frame buffer overflow as well as other reasons
transmitPktsDroppedInternalCongestion	(G-Series only) The number of frames dropped in the transmit direction due to frame buffer overflow as well as other reasons
txTotalPkts	Total number of transmit packets
rxTotalPkts	Total number of receive packets
mediaIndStatsOversizeDropped	Number of received packets larger than the CE-100T-8 remote monitoring (RMON) threshold.
mediaIndStatsTxFramesTooLong	Number of packets transmitted that are greater than 1548

Table 22-7 POS Threshold Variables (MIBs)

Variable	Definition
ifInPayloadCrcErrors	Number of CRC errors in the frame inside the GFP/HDLC payload coming in from the SONET receive (RX) direction.
ifOutPayloadCrcErrors	Number of CRC errors in the frame inside the GFP/HDLC payload coming in from the SONET transmit (TX) direction
ifOutOversizePkts	Number of packets larger than 1518 bytes sent out into SONET. Packets larger than 1600 bytes do not get transmitted.
etherStatsDropEvents	Number of received frames dropped at the port level.
gfpStatsRxSBitErrors	Receive frames with Single Bit Errors (cHEC, tHEC, eHEC)
gfpStatsRxMBitErrors	Receive frames with Multi Bit Errors (cHEC, tHEC, eHEC)

Table 22-7 POS Threshold Variables (MIBs) (continued)

Variable	Definition
gfpStatsRxTypeInvalid	Receive frames with invalid type (PTI, EXI, UPI)
gfpStatsRxCRCErrors	Receive data frames with Payload cyclic redundancy check (CRC) errors
gfpStatsRxCIDInvalid	Receive frames with Invalid CID
gfpStatsCSFRaised	Number of receive (Rx) client management frames with Client Signal Fail indication.
gfpStatsRxFrame	Receive data frames
gfpStatsTxFrame	Transmit data frames
gfpStatsRxOctets	Received data Octets
gfpStatsTxOctets	Transmit data Octets

Step 7 From the Alarm Type drop-down list, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

Step 8 From the Sample Type drop-down list, choose either **Relative** or **Absolute**. Relative restricts the threshold to use the number of occurrences in the user-set sample period. Absolute sets the threshold to use the total number of occurrences, regardless of time period.

Step 9 Type in an appropriate number of seconds for the Sample Period.

Step 10 Type in the appropriate number of occurrences for the Rising Threshold.

For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a rising threshold of 1000 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, the excess occurrences trigger an alarm.

Step 11 Enter the appropriate number of occurrences in the Falling Threshold field. In most cases a falling threshold is set lower than the rising threshold.

A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 minutes subsides and creates only 799 collisions in 15 minutes, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15-minute period, an event again triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded (otherwise, a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

Step 12 Click **OK** to complete the procedure.

Step 13 Return to your originating procedure (NTP).

DLP-A534 Provision OSI Routing Mode

Purpose	This task provisions the Open System Interconnection (OSI) routing mode. Complete this task when the ONS 15454 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	NTP-A323 Verify Card Installation, page 4-2
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, IS Level 1, or IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15454 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 For ONS 15454 nodes, three virtual routers can be provisioned. The node 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 Complete the "DLP-A60 Log into CTC" task on page 17-67 at the node where you want to provision the OSI routing mode. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > OSI > Main Setup** tabs.

Step 3 Choose a routing mode:

- End System—The ONS 15454 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 15454 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.

- Intermediate System Level 1/Level 2—The ONS 15454 performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. Before choosing this option, verify the following:
  - The node is connected to another IS Level 1/Level 2 node that resides in a different OSI area.
  - The node is connected to all nodes within its area that are provisioned as IS L1/L2.

Step 4 If needed, change the LSP data buffers:

- L1 LSP Buffer Size—Adjusts the Level 1 link state PDU buffer size. The default is 512. It should not be changed.
- L2 LSP Buffer Size—Adjusts the Level 2 link state PDU buffer size. The default is 512. It should not be changed.

Step 5 Return to your originating procedure (NTP).

DLP-A535 Provision or Modify TARP Operating Parameters

Purpose	This task provisions or modifies the Target Identifier Address Resolution Protocol (TARP) operating parameters including TARP protocol data unit (PDU) propagation, timers, and loop detection buffer (LDB).
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-67
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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 The TARP PDUs L1 Propagation parameter is not used when the Node Routing Area (Provisioning > OSI > Main Setup tab) is set to End System.

- TARP PDUs L2 Propagation—If checked (default), TARP Type 2 PDUs received by the node that are not excluded by the LDB are propagated to other NEs within the Level 2 OSI areas. (Type 2 PDUs request a protocol address that matches a TID within a Level 2 routing area.) The propagation occurs if the NE is not the target of the Type 2 PDU, and PDUs are not propagated to the NE from which the PDU was received.

Note The TARP PDUs L2 Propagation parameter is only used when the Node Routing Area is provisioned to Intermediate System Level 1/Level 2.

- 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 and NSAP to TID 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.

- L2 TARP Data Cache—If checked (default), the TIDs and NSAPs of NEs originating Type 2 requests are added to the TDC before the node propagates the requests to other NEs.

The TARP Data Cache parameter is designed for Intermediate System Level 1/Level 2 nodes that are connected to other Intermediate System Level 1/Level 2 nodes. Enabling the parameter for Intermediate System Level 1 nodes is not recommended.

- 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.

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 15454 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 The T1, T2, and T4 timers are not used if TARP PDUs Origination is not enabled.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-A536 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-A60 Log into CTC, page 17-67
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-A537 Remove a Static TID to NSAP Entry from the TARP Data Cache

Purpose	This task removes a static TID to NSAP entry from the TDC.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-67
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-A538 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 15454 must communicate across routers or non-SONET NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-67
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-A539 Provision OSI Routers

Purpose	This task enables an OSI router and edits its primary manual area address.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Router 1 must be enabled before you can enable and edit the primary manual area addresses for Routers 2 and 3.

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. The System IDs for Routers 2 and 3 are created by adding 1 and 2 respectively to the Router 1 System ID. You cannot edit the System IDs.

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

Step 2 Chose the router you want provision 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 **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-A540 Provision Additional Manual Area Addresses

Purpose	This task provisions the OSI manual area addresses. One primary and two additional manual areas can be created for each virtual router.
Tools/Equipment	None
Prerequisite Procedures	DLP-A539 Provision OSI Routers, page 22-45 DLP-A60 Log into CTC, page 17-67
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 Chose the router where you want provision an additional manual area address and click **Edit**. The OSI Router Editor dialog box.

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-A541 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-A60 Log into CTC, page 17-67
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-A377 Provision Section DCC Terminations" task on page 20-68 and the "DLP-A378 Provision Line DCC Terminations" task on page 20-70.

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 15454 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-A542 Create an IP-Over-CLNS Tunnel

Purpose	This task creates an IP-over-CLNS tunnel to allow ONS 15454s to communicate across equipment and networks that use the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
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 15454. The other end point is generally provisioned on non-ONS equipment including routers and other network elements (NE). Before you begin, verify that you have the capability to create an OSI over IP 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 OSI 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.

- 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 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 using the documentation.

Step 6 Return to your originating procedure (NTP).

DLP-A543 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-A60 Log into CTC, page 17-67
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-A544 Change the OSI Routing Mode

Purpose	This task changes the OSI routing mode.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-67
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, IS Level 1, or IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15454 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 Verify the following:

- All L1/L2 virtual routers on the NE must reside in the same area. This means that all neighboring virtual routers must have at least one common area address.
- For OSI L1/L2 to ES routing mode changes, only one L1/L2 virtual router and no more than one subnet can be configured.
- For OSI L1 to ES routing mode changes, only one L1 virtual router and no more than one subnet can be configured.

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

Step 3 Choose one of the following routing modes:

- **End System**—The ONS 15454 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.
- **Intermediate System Level 1/Level 2**—The ONS 15454 performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. Before choosing this option, verify the following:
  - The node is connected to another IS Level 1/Level 2 node that resides in a different OSI area.
  - The node is connected to all nodes within its area that are provisioned as IS L1/L2.

Note Changing a routing mode should be carefully considered. Additional information about OSI ESs and ISs and the ES-IS and IS-IS protocols are provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 4 Although Cisco does not recommend changing the LSP (Link State Protocol Data Unit) buffer sizes, you can adjust the buffers in the following fields:

- L1 LSP Buffer Size—Adjusts the Level 1 link state PDU buffer size.
- L2 LSP Buffer Size—Adjusts the Level 2 link state PDU buffer size.

Step 5 Return to your originating procedure (NTP).

DLP-A545 Edit the OSI Router Configuration

Purpose	This task allows you to edit 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-A60 Log into CTC, page 17-67
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 Chose 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-A546 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-A60 Log into CTC, page 17-67
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 > 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.

Click **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-A547 Edit an IP-Over-CLNS Tunnel

Purpose	This task allows you to edit the parameters of an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-A542 Create an IP-Over-CLNS Tunnel, page 22-47 DLP-A60 Log into CTC, page 17-67
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 In node view, 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—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.

- 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-A548 Delete an IP-Over-CLNS Tunnel

Purpose	This task allows you to delete an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-67
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 In node view, 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-A549 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-A60 Log into CTC, page 17-67
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the 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 NSAP (network service access point) of the IS.

- MAC Address—For destination NEs that are accessed by LAN subnets, the NE's Media Access Control 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-A550 View ES-IS Routing Information Base

Purpose	This task allows you to view the End System to Intermediate System (ES-IS) protocol routing information base (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-A60 Log into CTC, page 17-67
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 (network service access point).
- MAC Address—For destination NEs that are accessed by LAN subnets, the NE's Media Access Control 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-A551 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-A60 Log into CTC, page 17-67
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 Network Service Access Point or Network Element Title of the originating NE.
- Type—Indicates how the TARP data cache 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 TARP data cache is not enabled on the Provisioning > OSI > TARP subtab.

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

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

c. Click **OK**, then click **OK** on 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-A552 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-A596 Provision the Ethernet Port of the ML-Series Card

Purpose	This task provisions the Ethernet ports of the ML-Series card to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, double-click the ML-Series card where you want to provision the Ethernet port.

Step 2 Click the **Provisioning > Ether Ports** tabs.
The Ether Ports pane appears.

Step 3 In the Ether Ports pane complete the following:

- Port—Displays a fixed number identifier for the specific port.
- Port Name—Enter a 12 character alphanumeric identifier for the port.

Note Circuit table displays port name of the POS port and not the Ethernet port. For information on viewing the circuit table, see DLP-A416 View Circuit Information, page 21-2.

- Admin State—Displays the state of the port. Allowed values are UP and DOWN. For the UP value to appear, the Ethernet port must be both administratively active and have a SONET/SDH circuit provisioned.
- PSAS (Pre Service Alarm Suppress)—Check the PSAS checkbox to enable alarm suppression on the port for a time interval set in the Soak Time column. Uncheck the PSAS checkbox to disbale alarm suppression.

- Soak Time—Enter a desired soak time in hours and minutes (hh:mm) format. Use this column when you have checked PSAS to suppress alarms. Once the port detects a signal, the countdown begins for the designated soak time. Soak time hours can be set from 0 to 48. Soak time minutes can be set from 0 to 45 in 15 minute increments.
- Link State—Displays the status between signaling points at port and attached device. Allowed values are UP or DOWN.
- MTU (Maximum Transmission Unit)— Displays the largest acceptable packet size configured for the port.
- Speed—Displays the Ethernet port transmission speed.
- Duplex—Displays the duplex mode setting for the port.
- Flow Control—Displays the flow control mode negotiated with peer device.
- Optics— Displays the Small form-factor pluggable (SFP) physical media type.

Step 4 Click **Apply.**

Step 5 Reprovisioning an Ethernet port on the ML-Series card does not reset the ethernet statistics for that port. The Ethernet Statistics must be refreshed. To do so, do the following:

a. Click the **Performance** > **Ether Ports** > **Statistics** tabs.

b. Click **Refresh.**

Step 6 Return to your originating procedure (NTP).

DLP-A597 Provision the POS Port of the ML-Series Card

Purpose	This task provisions the POS ports of the ML-Series card to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, double-click the ML-Series card where you want to provision the POS port.

Step 2 Click the **Provisioning** > **POS Ports** tabs.
The POS Port pane appears.

Step 3 For each port, provision the following parameters:

- Port—Displays a fixed number identifier for the specific port.
- Port Name—Enter a 12 character alphanumeric identifier for the port.

Note Circuit table displays port name of the POS port and not the Ethernet port. For information on viewing the circuit table, see DLP-A416 View Circuit Information, page 21-2.

- Admin State—Displays the state of the port. Allowed values are UP or DOWN. For the UP value to appear, a POS port must be both administratively active and have a SONET/SDH circuit provisioned.
- PSAS—Check the PSAS checkbox to enable alarm suppression on the port for a time interval set in the Soak Time column. Uncheck the PSAS checkbox to disbale alarm suppression.
- Soak Time—Enter a desired soak time in hours and minutes (hh:mm) format. Use this column when you have checked PSAS to suppress alarms. Once the port detects a signal, the countdown begins for the designated soak time. Soak time hours can be set from 0 to 48. Soak time minutes can be set from 0 to 45 in 15 minute increments.
- Link State—Displays the status between signaling points at port and attached device. Allowed values are UP or DOWN.
- MTU—Displays the largest acceptable packet size configured for the port.
- Framing Type— Displays the POS framing mechanism employed on the port.

Step 4 Click **Apply.**

Step 5 Reprovisioning a POS port on the ML-Series card does not reset the POS statistics for that port. The POS Statistics must be refreshed. To do so, do the following:

a. Click the **Performance > POS Ports > Statistics** tabs.

b. Click **Refresh.**

Step 6 Return to your originating procedure (NTP).