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.

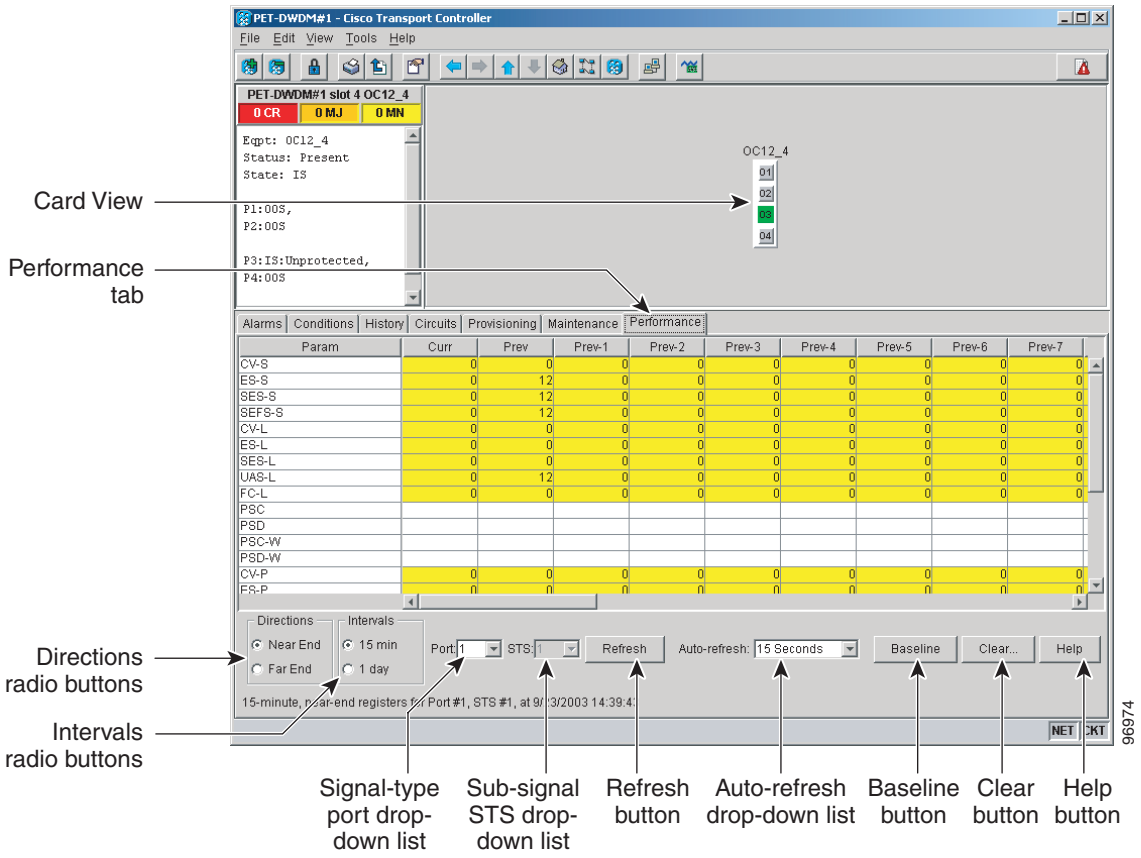
DLP-A507 View OC-N PM Parameters

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 17-66
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 Troubleshooting Guide*.

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-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 17-66
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, 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 the map DS-3 circuit to an STS.

Step 8 Depending on the destination card, choose the destination port or STS from the submenus 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, VTs, or DS3s if they are already in use by other circuits. If you and a user 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-A511 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 performance monitoring data.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66
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—Sets 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.
  - **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:

- **Telnet**—If chosen, allows access to the node using Telnet. Telnet is the terminal-remote host Internet protocol developed for the Advanced Agency Research Project Network (ARPANET). If chosen, choose the Telnet port. Port 23 is the default.
- **SSH**—If chosen, allows access to the node using the Secure Shell (SSH) program. SSH is a terminal-remote host Internet protocol that uses encrypted links. If chosen, Port 22 is the default port. It cannot be changed.

Step 4 In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: **RETRIEVE**, **PROVISIONING**, **MAINTENANCE**, or **SUPERUSER**.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A515 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 17-66
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**.

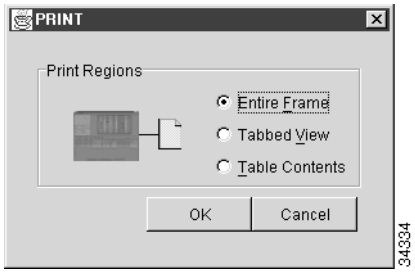
Step 3 In the Print dialog box, click a printing option (Figure 22-2).

- **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 applies to all windows except:
  - Provisioning > General > General and Power Monitor windows
  - Provisioning > Network > General and RIP windows
  - Provisioning > Security > Policy, Access, and Legal Disclaimer windows
  - Provisioning > SNMP window
  - Provisioning > Timing window
  - Provisioning > UCP > Node window
  - Provisioning > WDM-ANS > Provisioning 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 the 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 the network view does not contain an Inventory tab or Performance tab.

Figure 22-2 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-A516 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.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-66
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).

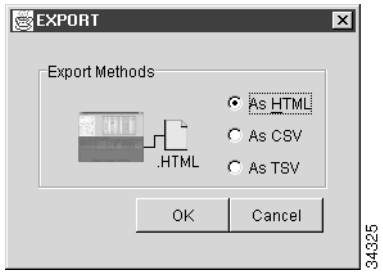
Step 2 From the File menu, choose **Export**.

Step 3 In the Export dialog box, click a data format (Figure 22-3):

- **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 22-3 Selecting CTC Data For Export



Step 4 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 5 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 applies to all tabular data except:

- Provisioning > General > General and Power Monitor windows
- Provisioning > Network > General and RIP windows
- Provisioning > Security > Policy, Access, and Legal Disclaimer windows
- Provisioning > SNMP window
- Provisioning > Timing window
- Provisioning > UCP > Node window
- Provisioning > WDM-ANS > Provisioning window
- Maintenance > Cross-Connect > Cards window
- Maintenance > Database window
- Maintenance > Diagnostic window
- Maintenance > Protection window
- Maintenance > Timing > Source and Report windows

Step 6 Click **OK**.

Step 7 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 8 Navigate to a directory where you want to store the file.

Step 9 Click **OK**.

Step 10 Repeat the task for each window that you want to export.

Step 11 Return to your originating procedure (NTP).

DLP-A517 View Alarm or Event History

Purpose	This task is used to view previously 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 17-66
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 > Node** 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 > Node tabs.

Note Alarms might be unreported if 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/TCC2P cards and cross-connect (XCVT or XC10G) 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 17-66
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. The node view is shown in Figure 7-2 on page 7-5.

Step 3 To access the profile editor from a card view, click the following tabs:

- If the card is an FC_MR-4, E-Series Ethernet, G-Series Ethernet, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3N, DS3-12E, DS3-12E-N, DS3i, DS3i-N, DS3XM, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Behavior** tabs to apply the profile to the front physical ports, or the **Provisioning > POS Alarming > Alarm Behavior** tabs to apply the profile to the packet-over-SONET (POS) ports.

For more information about ML-Series card ports and service, see the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454 SDH, Cisco ONS 15454, and Cisco ONS 15327*.

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:

a. Click **Load** and **From Node** in the Load Profile(s) dialog box.

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

c. 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 that is stored as a file locally or on a network drive:

a. Click **From File** in the Load Profile(s) dialog box.

b. Click **Browse**.

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

d. 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 alarm severity profile appears in the Alarm Profiles window.

Note 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, refer to 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 CR or MJ default or user-defined severity settings are demoted to MN in 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 If you want to store the profile on a node:

a. In the Store Profile(s) dialog box (Figure 22-4), click **To Node(s)**.

b. Choose the node(s) 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**.

c. If you want to update alarm profile information, click **(Synchronize)**.

Step 16 If you want to save the profile to a file:

a. In the Store Profile(s) dialog box (Figure 22-4), click **To File**.

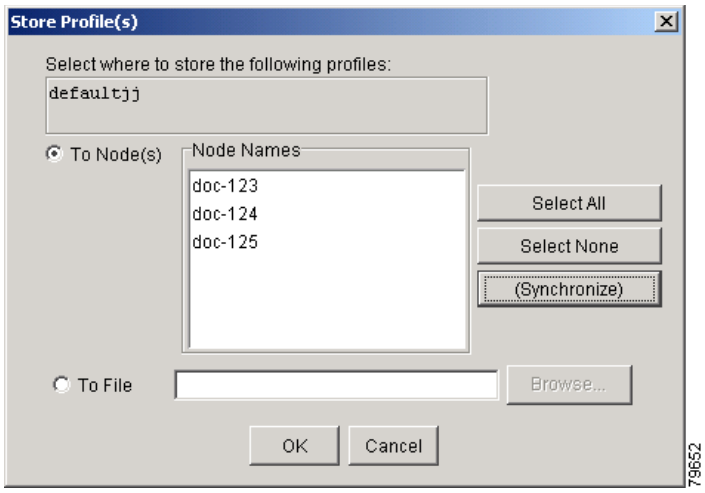
b. Click **Browse** and navigate to the profile save location.

c. Enter a name in the File name field.

d. Click **Select** to choose this name and location.

Note Long file names are supported. CTC supplies a suffix of *.pfl to stored files.

Figure 22-4 Store Profiles Dialog Box



Step 17 Click **OK** to store the profile.

Note Click the **Hide Identical Rows** check box to configure the Alarm Profiles window to view rows with dissimilar severities.

Note Click the **Hide Reference Values** check box to configure the Alarm Profiles window to view severities that do not match the Default profile.

Note 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 18 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 22-9 DLP-A60 Log into CTC, page 17-66
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.

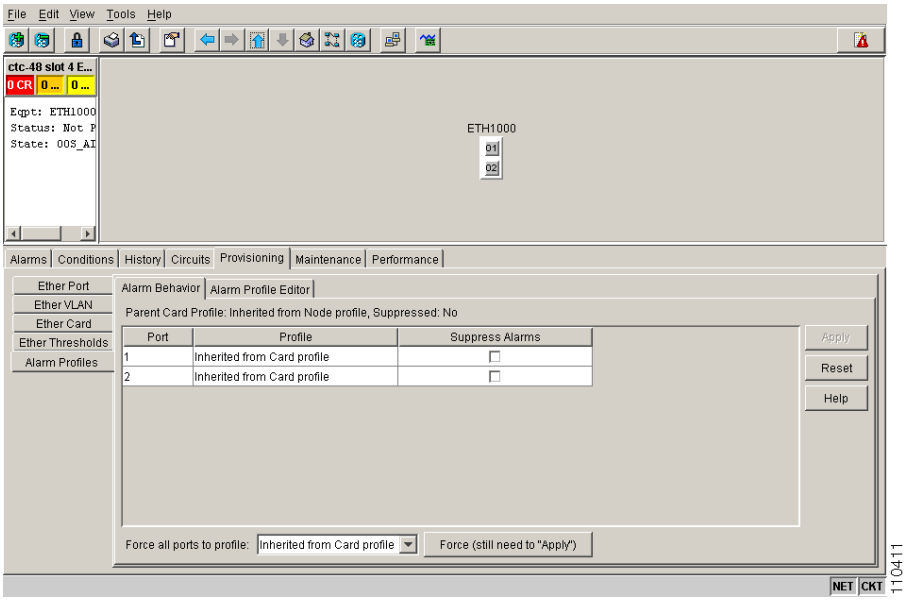
Note The card view is not available for the TCC2/TCC2P or cross-connect cards.

Step 2 Depending on which card you want to apply the profile to, click the following tabs:

- If the card is an FC_MR-4, E-Series Ethernet, G-Series Ethernet, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS3i, DS3i-N, DS-3N, DS-3NE, DS3XM, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Behavior** tabs to apply the profile to the front physical ports, or the **Provisioning > POS Alarming > Alarm Behavior** tabs to apply the profile to the POS ports. For more information about ML-Series card ports and service, see the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454 SDH, Cisco ONS 15454, and Cisco ONS 15327*.

Figure 22-5 shows the alarm profile for the ports of an E-Series Ethernet card. CTC shows that the parent card profile is Inherited.

Figure 22-5 E-Series Card Alarm Profile



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, choose a new profile from the **Force all ports to profile** drop-down list at the bottom of the window.

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

c. Click **Apply**.

In node view, the Port Level Profiles column indicates port-level profiles with a notation such as "exist (1)" (for an example, see 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 17-66
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, click the following tabs:

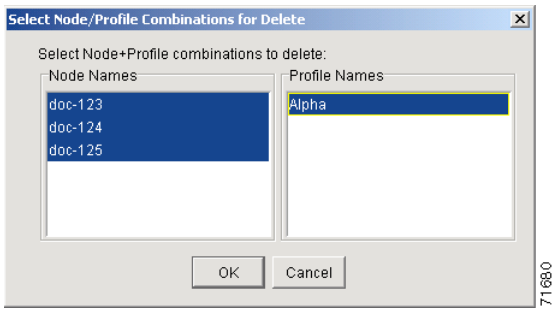
- If the card is an FC_MR-4, E-Series Ethernet, G-Series Ethernet, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS3i, DS3i-N, DS-3N, DS-3NE, DS3XM, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Behavior** tabs to apply the profile to the front physical ports, or the **Provisioning > POS Alarming > Alarm Behavior** tabs to apply the profile to the POS ports. For more information about ML-Series card ports and service, see the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454 SDH, Cisco ONS 15454, and Cisco ONS 15327*.

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 22-6).

Figure 22-6 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 name(s) in the Node Names list to highlight the profile location.

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

Step 7 Click the profile name(s) 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 dialog box.

Step 10 Return to your originating procedure (NTP).

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

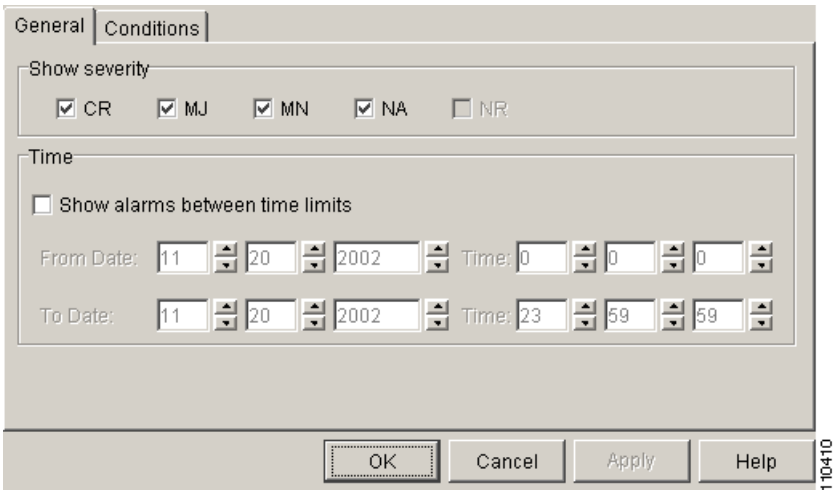
Purpose	This task changes alarm and condition reporting in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A225 Enable Alarm Filtering, page 19-17 DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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 22-7 shows the Alarm Filter dialog box; the Conditions and History tabs have similar dialog boxes.

Figure 22-7 Alarm Filter Dialog Box General Tab



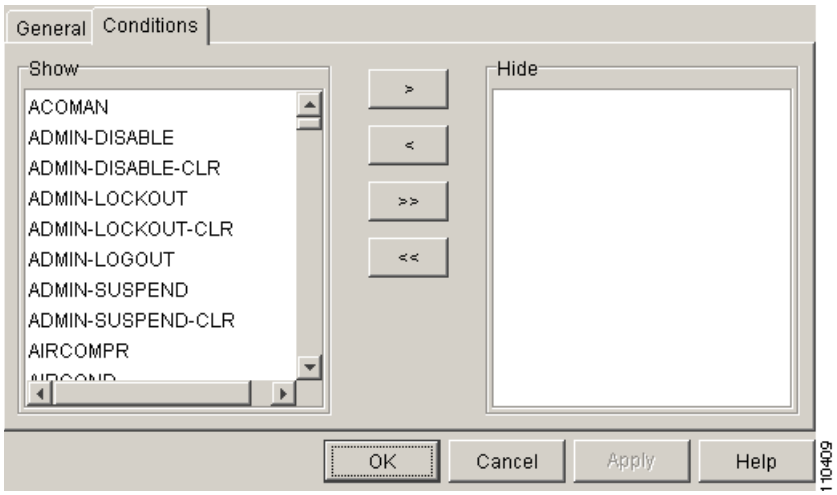
Step 3 In the Show Severity area, click the check boxes for the severities [**CR**, **MJ**, **MN**, or Not-Alarmed (**NA**)] that you want to show through the alarm filter and be reported at the network level. Leave severity check boxes deselected (unchecked) to prevent those severities from appearing.

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 the period of alarms that is shown.

Step 5 To modify filter parameters for conditions, click the filter dialog box **Conditions** tab (Figure 22-8). If you do not need to modify them, continue with Step 6.

Figure 22-8 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 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 17-66
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 User Command (AS-CMD) alarm.

Step 1 To suppress alarms for the entire node:

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

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

c. 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 building integrated timing supply (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 2 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 1. 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 3 To suppress alarms for individual card ports:

a. Double-click the card in node view. Depending on which card ports you want to suppress alarm reporting on, click the following tabs:

- If the card is an FC_MR-4, E-Series Ethernet, G-Series Ethernet, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, DS3XM, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Behavior** tabs to apply the profile to the front physical ports, or the **Provisioning > POS Alarming > Alarm Behavior** tabs to apply the profile to the POS ports. For more information about ML-Series card ports and service, see the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454 SDH, Cisco ONS 15454, and Cisco ONS 15327*.

b. Check the **Suppress Alarms** column check box for the row of the port where you want to suppress alarms (Figure 22-5 on page 22-13).

c. Click **Apply**.

Alarms that apply directly to this port will change appearance as described in Step 1. (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 4 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 22-17 DLP-A60 Log into CTC, page 17-66
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:

a. Click the following tabs:

- If the card is an FC_MR-4, E-Series Ethernet, G-Series Ethernet, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS3i, DS3i-N, DS-3N, DS-3NE, DS3XM, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Behavior** tabs to apply the profile to the front physical ports, or the **Provisioning > POS Alarming > Alarm Behavior** tabs to apply the profile to the POS ports. For more information about ML-Series card ports and service, see the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454 SDH, Cisco ONS 15454, and Cisco ONS 15327*.

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

c. 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 4 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 17-66
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.
- From node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
- From the card view of an FC_MR-4, E-Series Ethernet, G-Series Ethernet, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS3i, DS3i-N, DS-3N, DS-3NE, DS3XM, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
- From the card view of an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Behavior** tabs to apply the profile to the front physical ports, or the **Provisioning > POS Alarming > Alarm Behavior** tabs to apply the profile to the POS ports. For more information about ML-Series card ports and service, see the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454 SDH, Cisco ONS 15454, and Cisco ONS 15327*.

Step 2 Click **Load**.

Step 3 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 4 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 CR or MJ are demoted to MN in NSA situations as defined in Telcordia GR-474.

Step 5 Click **OK**.

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

Step 6 Right-click anywhere in the downloaded profile column to view the profile editing shortcut menu.

Step 7 Click **Store**.

Step 8 In the Store Profile(s) dialog box, click **To Node(s)**.

a. Choose the node(s) 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 9 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 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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 7, "Manage Alarms" for information about the Alarm Behavior tab.

Step 4 Modify any of the settings found under these subtabs. For definitions of the line settings, see Table 22-1. For definitions of the line threshold settings, see Table 22-2. For definitions of the electrical path threshold settings, see Table 22-3. For definitions of the SONET threshold settings, see Table 22-4.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

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.) Shows the 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	(Display only.) Displays the detected line type.	• M13 • C Bit • Unframed • Unknown
Line Coding	(Display only.) Defines the DS3E transmission coding type.	B3ZS

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

Parameter	Description	Options
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
Admin State	Sets the port service state unless network conditions prevent the change.	• IS—Puts the port in service. The port service state changes to In-Service and Normal (IS-NR). • IS,AINS—Puts the port in automatic in-service. The port service state changes to Out-Of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS). • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to Out-of-Service and Management, Disabled (OOS-MA,DSBLD). • OOS,MT—Removes the port from service for maintenance. The port service state changes to Out-of-Service and Management, Maintenance (OOS-MA,MT).
Service State	Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—The port is fully operational and performing as provisioned. • OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. • OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
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 values 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	Options
Port	(Display only.) Port number	1 to 12
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button.

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

Parameter	Description	Options
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button.
LOSS	Loss of signal seconds; number of one-second intervals containing one or more LOS defects	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button.

Table 22-3 describes the values 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	Options
Port	(Display only.) Port number	1 to 12
CVP	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
ESP	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
SESP	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
SASP	Severely errored frame/alarm indication signal–path	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
UASP	Unavailable seconds–path	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
AISSP	Alarm indication signal seconds–path	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).

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	Options
Port	(Display only.) Port number	1 to 12
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (STS and VT Term).
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, Sts Term or Vt Term).
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals for Line or Path (Near and Far End). Select the bullet and click **Show Thresholds**.

Note The threshold value appears after the circuit is created.

Step 7 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 17-66
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 Choose a default map from the **Default Value** drop-down list. Map choices are: **Germany**, **Japan**, **Netherlands**, **South Korea**, **United Kingdom**, and **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 22-28 DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15454 ML-Series card uses the Cisco IOS CLI for managing 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 > RMON Thresholds** tabs.

Note For the CE-Series cards, 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).

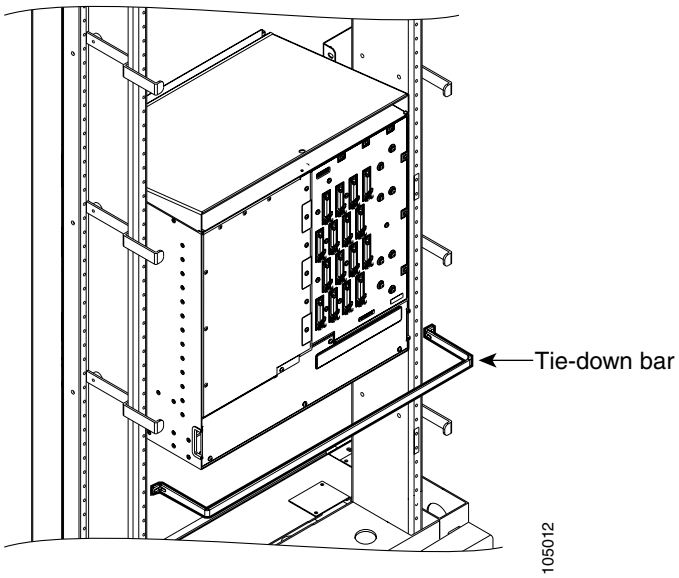
DLP-A530 Install the Tie-Down Bar

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 rack unit (RU) below the ONS 15454.

Figure 22-9 shows the tie-down bar, the ONS 15454, and the rack.

Figure 22-9 Tie-Down Bar



Step 2 Install the four screws into the rack.

Step 3 Return to your originating procedure (NTP).

DLP-A533 Create Ethernet RMON Alarm Thresholds

Purpose	This procedure sets up RMON to allow network management systems to monitor Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15454 ML-Series card uses the Cisco IOS CLI for managing RMON.

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

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

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

Step 3 Click **Create**.

The Create Ether Threshold dialog box appears (Figure 22-10).

Figure 22-10 Creating RMON Thresholds

Step 4 From the Slot drop-down list, choose the appropriate Ethernet card.

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 22-5 and Table 22-6 for a list of the Ethernet and POS threshold variables available in this field.

Table 22-5 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 frame check 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 22-5 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 Physical Layer Switch (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 coaxial segments to which the repeater is connected.

Table 22-5 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 (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 coaxial 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	Total number of good packets received that were directed to a multicast address, not including packets directed to the broadcast
etherStatsOversizePkts	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 22-5 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.) Number of received IEEE 802.x pause frames
transmitPauseFrames	(G-Series only.) Number of transmitted IEEE 802.x pause frames
receivePktsDroppedInternalCongestion	(G-Series only.) Number of received frames dropped due to frame buffer overflow as well as other reasons
transmitPktsDroppedInternalCongestion	(G-Series only.) 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 RMON threshold.
mediaIndStatsTxFramesTooLong	Number of packets transmitted that are greater than 1548

Table 22-6 POS Threshold Variables (MIBs)

Variable	Definition
ifInPayloadCrcErrors	Number of cyclic redundancy check (CRC) errors in the frame inside the generic framing protocol/high-level data link control (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)

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

Variable	Definition
gfpStatsRxMBitErrors	Receive frames with multi bit errors (cHEC, tHEC, eHEC)
gfpStatsRxTypeInvalid	Receive frames with invalid type (PTI, EXI, UPI)
gfpStatsRxCRCErrors	Receive data frames with Payload CRC errors
gfpStatsRxCIDInvalid	Receive frames with Invalid CID
gfpStatsCSFRaised	Number of 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 in the Sample Period field.

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

Note 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 minutes and a problem causes 1001 collisions in 15 minutes, 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.

Note 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-A553 Upgrade Low-Density Electrical Cards in a 1:N Configuration to High-Density Electrical Cards

Purpose	This task upgrades low-density electrical cards in a 1:N protection scheme (where N = 1 or 2) to high-density electrical cards (the DS3/EC1-48 card). Low-density cards are defined any of the following: DS-1, 12-port DS-3, and 12-port EC-1).
Tools/Equipment	DS3/EC1-48 cards High-density shelf assembly (15454-SA-HD) High-density EIA (MiniBNC, UBIC-V, UBIC-H) installed
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Protect cards must be upgraded before working cards because working cards cannot have more capabilities than their protect card.

Note You cannot upgrade electrical cards from low-density to high-density if the low-density electrical cards are installed in Slots 4, 5, or 6 (or 12, 13, or 14 on the B side of the shelf). Only cards in Slots 1, 2, 16, and 17 can be upgraded to high-density electrical cards.

Note This procedure describes an upgrade of Slots 1, 2, and 3 (15, 16, and 17) to high-density electrical cards. However, you can have any combination of low-density (12-port) electrical cards and high-density cards in Slots 1 and 2 (16 and 17) after you upgrade the protect card (Slot 3 or 15) to a high-density electrical card.

Note During the upgrade some minor alarms and conditions appear and then clear on their own; however, there should be no Service-Affecting (SA, Major, or Critical) alarms if you are upgrading protected cards. (Upgrading an unprotected card can be service affecting.) If any service-affecting alarms occur, Cisco recommends backing out of the procedure.

Note You cannot have any DS-1 cards installed on the same side of the shelf as the DS3/EC1-48 card when you finish the low-density to high-density upgrade.

Step 1 Determine which low-density card(s) (DS-1, DS-3, DS-3E) you want to upgrade to high-density, according to slot limitations.

The following limitations apply if you are upgrading a low-density protect card:

- The protect card must be in a protection group.

- The protect card must not protect any low-density electrical cards in Slots 4, 5, or 6 if on the A side of the shelf (Slots 12, 13, or 14 if on the B side).
- For 1:N protection groups where N = 2: On the A side, the protect card cannot be upgraded if any electrical cards are installed or preprovisioned in Slots 4, 5, or 6 (or Slots 12, 13, or 14 on the B side).
- For 1:N protection groups where with N = 1: On the A side, if the protect card is installed in Slot 3 and it protects a low-density card in Slot 1, the protect card cannot be upgraded if Slot 5 or 6 has an electrical card installed or preprovisioned. For the B side, if the protect card is installed in Slot 15 and it protects a low-density card in Slot 17, the protect card cannot be upgraded if Slot 12 or 13 has an electrical card installed or preprovisioned.
- For 1:N protection groups where N = 1: On the A side, if the protect card is installed in Slot 3 and it protects a low-density card in Slot 2, the protect card cannot be upgraded if an electrical card is installed or preprovisioned in Slot 4. On the B side, if the protect card is installed in Slot 15 and it protects a low-density card in Slot 16, the protect card cannot be upgraded if an electrical card is installed or preprovisioned in Slot 14.

The following limitations apply to upgrading a working card after you have upgraded the protect card:

- A working card in Slot 1 on the A side (Slot 17 if on the B side) cannot be upgraded if an electrical card is installed or preprovisioned in Slot 5 or 6 (Slot 12 or 13 on the B side).
- A working card in Slot 2 on the A side (Slot 16 if on the B side) cannot be upgraded if an electrical card is installed or preprovisioned in Slot 4 (Slot 14 on the B side).

Step 2 In node view, double-click the current protect card. The card view appears.

Slot 3 contains the protect card if you are working on the A side of the shelf, and Slot 15 contains the protect card if you are working on the B side of the shelf.

Step 3 Make sure the current protect card is not active:

a. In card view, click the **Maintenance > Protection** tabs.

b. Select the protection group where the protect card resides.

Step 4 If the card status is Protect/Active, perform a switch so that the protect card becomes standby:

a. Click on the card in the protection group list to highlight it.

b. Click **Switch.**

c. Click **Yes** in the confirmation dialog box.

Step 5 Physically remove the card:

a. Open the card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 6 In node view, right-click the protect slot (Slot 3 or Slot 15) and change the low-density card to the high-density card:

a. Choose **Change Card** from the drop-down list.

b. Choose the new card type (DS3/EC1-48) from the Change to drop-down list.

c. Click **OK**.

Step 7 Physically insert the new DS3/EC1-48 card into the protect slot:

a. Open the ejectors on the card.

b. Slide the card into the slot along the guide rails.

c. Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during DS3/EC1-48 card bootup, see the "NTP-A17 Install the Electrical Cards" procedure on page 2-8.

Step 8 To upgrade a low-density working card, switch traffic onto the protect card from the low-density card in Slot 1 if you are working on the A side, or Slot 17 if you are working on the B side:

a. In node view, double-click the card in Slot 1/Slot 17.

b. Click the **Maintenance > Protection** tabs.

c. Double-click the protection group that contains the card in Slot 1/Slot 17.

d. In the protection group list, click the card in Slot 1/Slot 17 to highlight it.

e. Click **Switch** and **Yes** in the Confirmation dialog box.

Step 9 Physically remove the low-density card in Slot 1/Slot 17:

a. Open the card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 10 In node view, change the low-density card to the high-density card in CTC:

a. Right-click Slot 1/Slot 17 and choose **Change Card** from the drop-down list.

b. Choose the new card type (DS3/EC1-48) from the Change to drop-down list.

c. Click **OK**.

Step 11 Insert the new DS3/EC1-48 card into Slot 1/Slot 17:

a. Open the ejectors on the card.

b. Slide the card into the slot along the guide rails.

c. Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during DS3/EC1-48 card bootup, see the "NTP-A17 Install the Electrical Cards" procedure on page 2-8.

Step 12 Clear the switch you performed in Step 8:

a. Double-click the card in Slot 1/Slot 17.

b. In the **Maintenance > Protection** tabs, double-click the protection group that contains the reporting card.

c. Click the card in the selected group to highlight the card.

d. Click **Clear** and click **Yes** in the confirmation dialog box.

The protect card in Slot 3 (A side) or Slot 15 (B side) should now become standby.

Step 13 Return to your originating procedure (NTP).

DLP-A554 Upgrade Low-Density Electrical Cards in a 1:1 Configuration to High-Density Electrical Cards

Purpose	This task upgrades low-density electrical cards (DS3XM-6 cards)) in a 1:1 protection scheme to high-density electrical cards (DS3XM-12 cards).
Tools/Equipment	DS3XM-12 cards High-density shelf assembly (15454-SA-HD) High-density EIA (MiniBNC, UBIC-V, UBIC-H) installed
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Protect cards must be upgraded before working cards because working cards cannot have more capabilities than their protect card.

Note You cannot upgrade electrical cards from low-density to high-density if the low-density electrical cards are installed in Slots 4, 5, or 6 (or 12, 13, or 14 on the B side of the shelf). Only cards in Slots 1, 2, 16, and 17 can be upgraded to high-density electrical cards.

Note During the upgrade some minor alarms and conditions appear and then clear on their own; however, there should be no Service-Affecting (SA, Major, or Critical) alarms if you are upgrading protected cards. (Upgrading an unprotected card can be service affecting.) If any service-affecting alarms occur, Cisco

Step 1 Determine which DS3XM-6 cards you want to upgrade to DS3XM-12, according to slot limitations.

Step 2 In node view, double-click the current protect card. The card view appears.

Step 3 Make sure the current protect card is not active:

a. In card view, click the **Maintenance > Protection** tabs.

b. Select the protection group where the protect card resides.

Step 4 If the card status is Protect/Active, perform a switch so that the protect card becomes standby:

a. Click on the card in the protection group list to highlight it.

b. Click **Switch.**

c. Click **Yes** in the confirmation dialog box.

Step 5 Physically remove the card:

a. Open the card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 6 In node view, right-click the protect slot and change the low-density card to the high-density card:

a. Choose **Change Card** from the drop-down list.

b. Choose the new card type (DS3XM-12) from the Change to drop-down list.

c. Click **OK**.

Step 7 Physically insert the new DS3XM-12 card into the protect slot:

a. Open the ejectors on the card.

b. Slide the card into the slot along the guide rails.

c. Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during DS3XM-12 card bootup, see the "NTP-A17 Install the Electrical Cards" procedure on page 2-8.

Step 8 To upgrade a low-density working card, switch traffic onto the protect card from the remaining low-density card in that 1:1 protect group:

a. In node view, double-click the remaining DS3XM-6 card from that 1:1 protect group.

b. Click the **Maintenance > Protection** tabs.

c. Double-click the protection group that contains that DS3XM-6 card.

d. In the protection group list, click the newly installed DS3XM-12 card ito highlight it.

e. Click **Switch** and **Yes** in the Confirmation dialog box.

Step 9 Physically remove the remaining DS3XM-6 card in that protect group:

a. Open the card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 10 In node view, change the DS3XM-6 card to a DS3XM-12 card in CTC:

a. Right-click the slot where the DS3XM-6 card resided and choose **Change Card** from the drop-down list.

b. Choose the new card type (DS3XM-12) from the Change to drop-down list.

c. Click **OK**.

Step 11 Insert the new DS3XM-12 card into the open slot:

a. Open the ejectors on the card.

b. Slide the card into the slot along the guide rails.

c. Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during DS3/EC1-48 card bootup, see the "NTP-A17 Install the Electrical Cards" procedure on page 2-8.

Step 12 Clear the switch you performed in Step 8:

a. Double-click the first DS3XM-12 card you installed.

b. In the **Maintenance > Protection** tabs, double-click the protection group that contains the reporting card.

c. Click the card in the selected group to highlight the card.

d. Click **Clear** and click **Yes** in the confirmation dialog box.

The protect card should now become standby.

Step 13 Return to your originating procedure (NTP).