Contents

DLP-D420 Install the Public-Key Security Certificate

Purpose	This task installs the ITU Recommendation X.509 public-key security certificate. The pubic-key certificate is required to run Software Release 4.1 or later.
Tools/Equipment	None
Prerequisite Procedures	This task is performed during the "DLP-D60 Log into CTC" task. You cannot perform it outside of this task.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. If the Java Plug-in Security Warning dialog box appears, choose one of the following options:
    - **Yes (Grant This Session)**-Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into the ONS 15454 SDH.
    - **No (Deny)**-Denies permission to install certificate. If you choose this option, you cannot log into the ONS 15454 SDH.
    - **Always (Grant Always)**-Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.
    - **More Details (View Certificate)**-Allows you to view the public-key security certificate.
2. If the Login dialog box appears, continue with Step 3. If the Change Java Policy File dialog box appears, complete this step. The Change Java Policy File dialog box appears if Cisco Transport Controller (CTC) finds a modified Java policy file (.java.policy) on your PC. In Software R4.0 and earlier, the Java policy file was modified to allow CTC software files to be downloaded to your PC. The modified Java policy file is not needed in ONS 15454 SDH nodes running Software R4.1 and later. Choose one of the following options:
    - **Yes**-Removes the modified Java policy file from your PC. Choose this option only if you will log into ONS 15454 SDH nodes running Software R4.1 software or later.
    - **No**-Does not remove the modified Java policy file from your PC. Choose this option if you will log into ONS 15454 SDH nodes running Software R4.0 or earlier. If you choose No, this dialog box will appear every time you log into the ONS 15454 SDH. If you do not want it to appear, check the **Do not show the message again** check box.

Caution! If you delete the Java policy file, you cannot log into nodes running Software R4.0 and earlier. If you delete the file and want to log into an ONS 15454 SDH running an earlier release, insert the software CD

for the release into your PC CD-ROM and run the CTC setup wizard to reinstall the Java policy file.

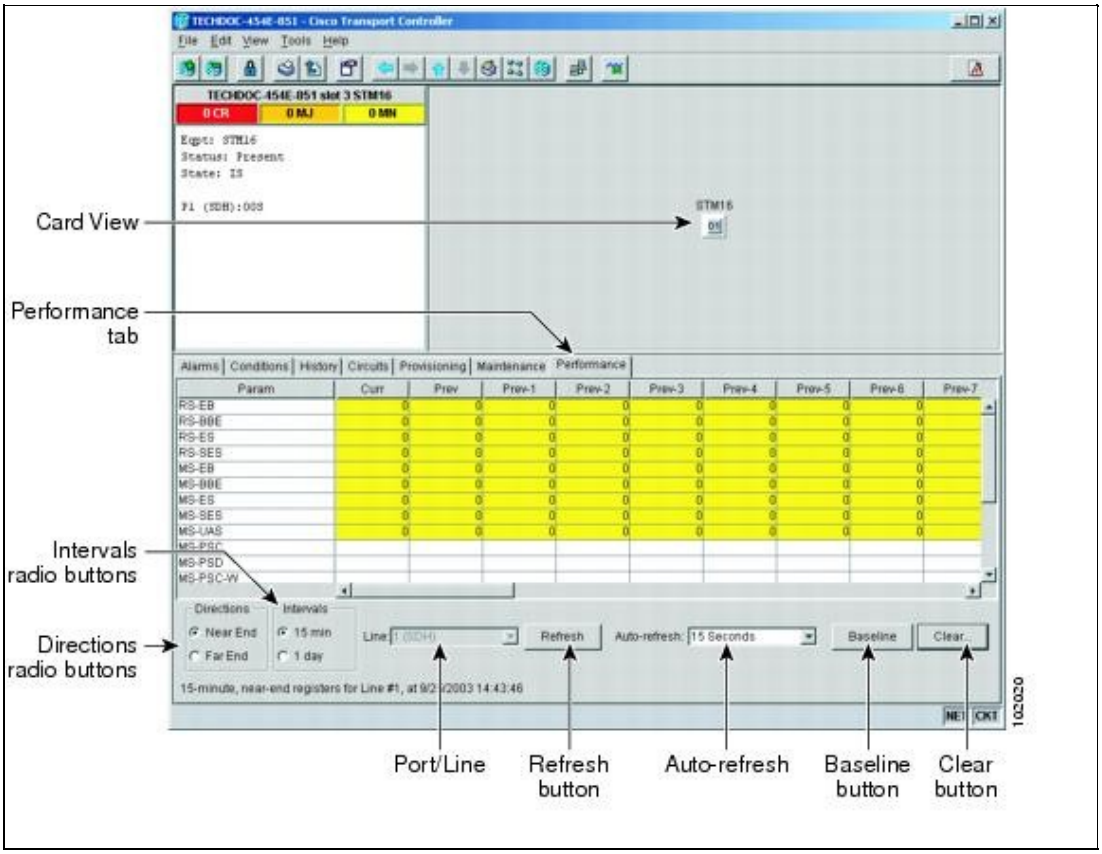
3. Return to your originating procedure (NTP).

DLP-D421 View STM-N PM Parameters

Purpose	This task enables you to view performance monitoring (PM) counts on an STM-N card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, double-click the STM-N card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab (Figure 21-1).

Figure 21-1: Viewing STM-N Card Performance Monitoring Information



3. From the Line drop-down list, choose the line you want to monitor.
4. Click **Refresh**.
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 SDH Reference Manual*.
6. To monitor another port on a multiport card, choose another line from the Line drop-down list and click **Refresh**.

7. Return to your originating procedure (NTP).

DLP-D422 Change the JRE Version

Purpose	This task changes the Java Runtime Environment (JRE) version, which is useful if you would like to upgrade to a later JRE version from an earlier one without using the software CD. This does not affect the browser default version. After selecting the desired JRE version, you must exit CTC. The next time you log into a node, the new JRE version will be used.
Tools	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. From the Edit menu, choose **Preferences**.
2. Click the **JRE** tab. The JRE tab shows the current JRE version and the recommended version.
3. Click the **Browse** button and navigate to the JRE directory on your computer.
4. Choose the JRE version.
5. Click **OK**.
6. From the File menu, choose **Exit**.
7. In the confirmation dialog box, click **Yes**.
8. Complete the "DLP-D60 Log into CTC" task.
9. Return to your originating procedure (NTP).

DLP-D424 View Alarm or Event History

Purpose	Use this task to view past cleared and uncleared ONS 15454 SDH 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-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note: Alarms can be unreported when they are filtered out of the display using the Filter button in either tab. See the "DLP-D225 Enable Alarm Filtering" task for information.

1. Decide whether you want to view the alarm message history at node, network, or card level.
2. To view node alarm history:
    1. Click the **History > Session** tabs to view the alarms and conditions (events) raised during the current session.
    2. Click the **History > Shelf** tabs to view the alarm and condition history for the node.
        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 alarms and events.
    3. Click **Retrieve** to view all available messages for the History > Shelf tab.

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.

3. To view network alarm history from node view:
    1. From the View menu, choose **Go to Network View**.
    2. Click the **History** tab.
       Alarms and conditions (events) raised during the current session appear.
4. To view card alarm history from node view:

    1. From the View menu, choose **Go to Previous View**.
5. Double-click a card on the shelf graphic to open the card-level view.

   Note: TCC2/TCC2P cards and cross-connect cards do not have a card view.
6. Click the **History > Session** tabs to view the alarm messages raised during the current session.
7. Click the **History > Card** tabs and click **Retrieve** to retrieve all available alarm messages for the card.

   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 alarms and events.
   Note: The ONS 15454 SDH 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 SDH discards the oldest events in that category.
   Raised and cleared alarm messages (and events, if selected) appear.

5. Return to your originating procedure (NTP).

DLP-D425 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-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. Access the alarm profile editor. To do this:
    - From network view, click the **Provisioning > Alarm Profiles** tabs. Figure 21-2 shows the network view.
    - From node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
    - From card view for an FC_MR-4, E-Series Ethernet, G-Series Ethernet, STM-N, or electrical (DS3i-N-12, E-1, E1-42, or E-3) card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
    - From card view for an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profile Editor** tabs or the **Provisioning > POS Alarming > Alarm Profile Editor** tabs, depending on whether you want to apply the profile to the front physical ports ("Ether alarming") or packet over SDH ("POS alarming"). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 and Cisco ONS 15454 SDH*

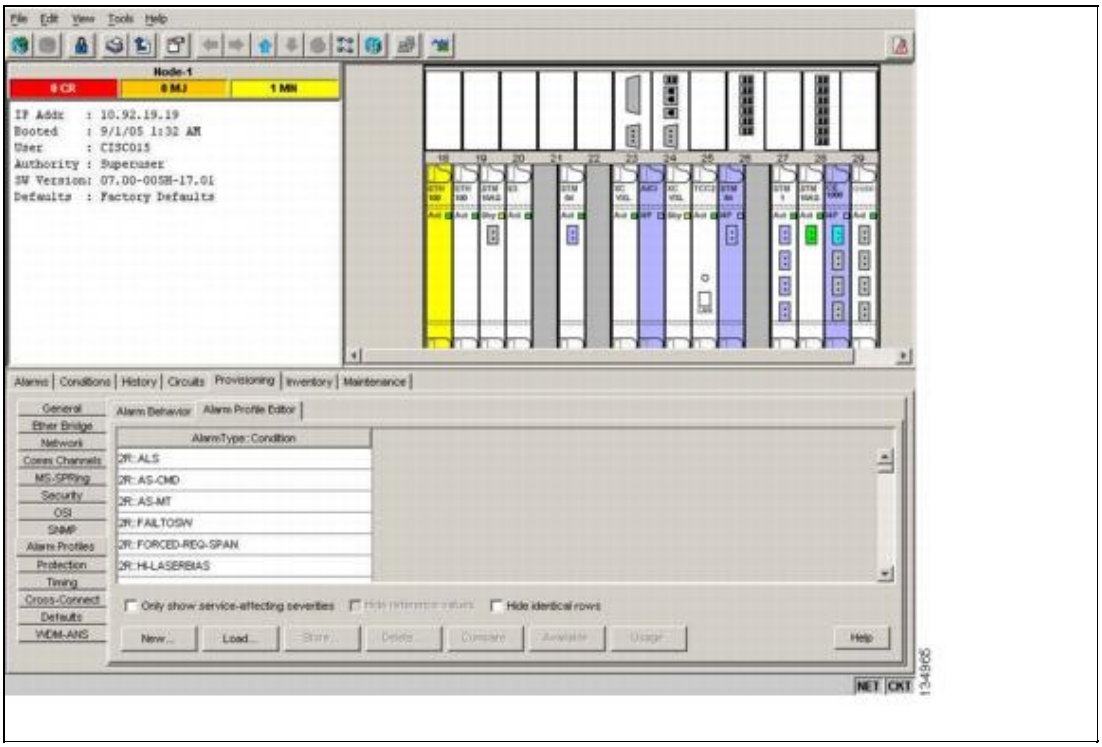
Ethernet Card Software Feature and Configuration Guide.

2. If you want to create a new profile based upon the default profile in use, click **New**. Then go to Step 8.
3. If you want to create a profile using an existing profile located on the node:
    1. Click **Load** and **From Node** in the Load Profile(s) dialog box.
    2. Click the node name you are logged into in the Node Names list.
    3. Click the name of an existing profile in the Profile Names list, such as **Default**. Then go to Step 5.
4. If you want to create a profile using an existing profile located in a file that is stored locally or on a network drive:
    1. Click **From File** in the Load Profile(s) dialog box.
    2. Click **Browse**.
    3. Navigate to the file location in the Open dialog box.
    4. 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.
5. Click **OK**.

    The alarm severity profile appears in the Alarm Profiles window (Figure 21-2). 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.

Figure 21-2: Network View Alarm Profiles Window



6. Right-click anywhere in the profile column to display the profile editing shortcut menu. (Refer to Step 9 for further information about the Default profile.)
7. Click **Clone** in the shortcut menu.

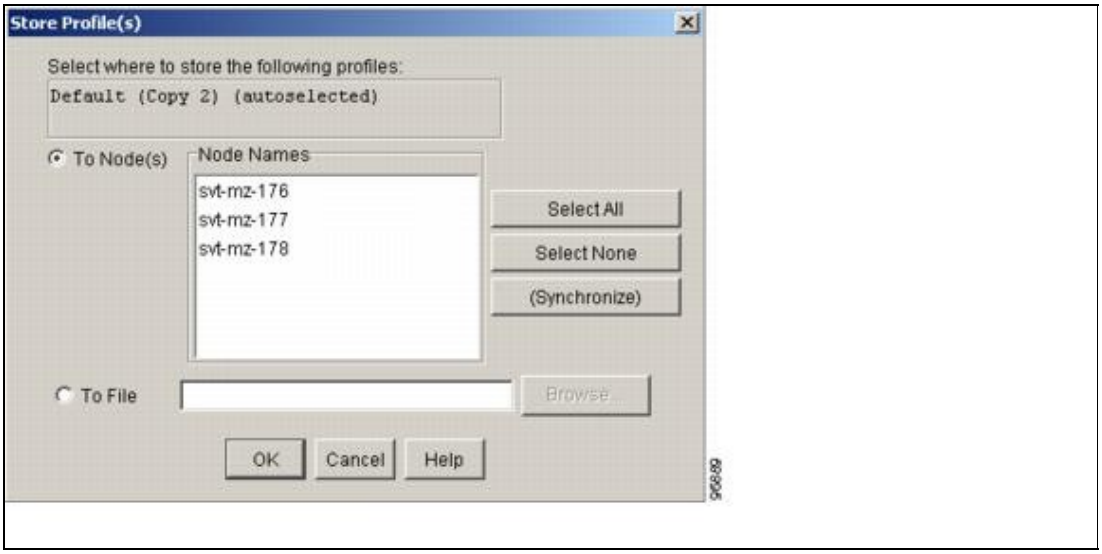
    Tip: To see the full list of profiles, including those available for loading or cloning, click **Available**. You must load a profile before you can clone it.
8. In the New Profile or Clone Profile dialog box, enter a name in the New Profile Name field.

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.

9. Click **OK**.

   A new alarm profile (named in Step 8) 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 ten profiles, including the two reserved profiles, Inherited and Default, can be stored in CTC.
   The Default profile sets severities to standard IEEE 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 profile copies the severities used by the node that contains the card. (If you are creating profiles, you can apply these separately at the network level or at the card level. To do this, refer to the "DLP-D117 Apply Alarm Profiles to Cards and Nodes" task.)
10. Modify (customize) the new alarm profile:
    1. In the new alarm profile column, double-click the alarm severity you want to change in the custom profile.
    2. Choose a severity from the drop-down list.
    3. Repeat Substeps 1 and 2 of Step 10 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.
    4. Default severities are used for all alarms and conditions until you create and apply a new profile.
    5. Changing a severity to inherited (I) or unset (U) does not change the severity of the alarm.
11. After you have customized the new alarm profile, right-click the profile column to highlight it.
12. Click **Store**.
13. If you want to save the profile to a node:
    1. In the Store Profile(s) dialog box, click **To Node(s)** (Figure 21-3).

Figure 21-3: Store Profile(s) Dialog Box



    2. If you want to save the profile to only one node, click the node in the Node Names list.
    3. If you want to save the profile to all nodes, click **Select All**.
    4. If you do not want to save the profile to any nodes, click **Select None**.

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

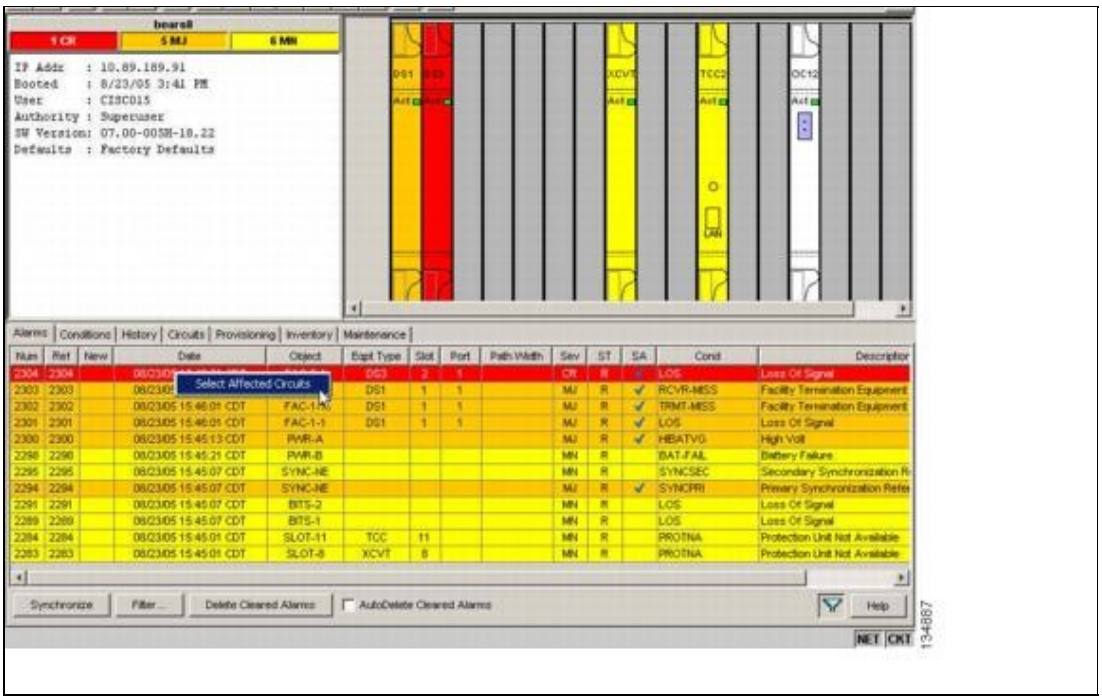
14. If you want to save the profile to a file:
    1. In the Store Profile(s) dialog box (Figure 21-3), click **To File**.
    2. Click **Browse** and navigate to the profile save location.
    3. Enter a name in the File name field.
    4. Click **Select** to choose this name and location. Long file names are supported. CTC supplies a suffix of *.pfl to stored files.
    5. Click **OK** to store the profile.
15. 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.
16. Return to your originating procedure (NTP).

DLP-D426 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-D425 Create a New or Cloned Alarm Severity Profile DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, double-click a card to open the card view.
   Note: You can also apply alarm profiles to cards using the "DLP-D117 Apply Alarm Profiles to Cards and Nodes" task.
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, STM-N, or electrical (DS3i-N-12, E-1, E1-42, or E-3) 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 Profile Editor** tabs or the **Provisioning > POS Alarming > Alarm Profile Editor** tabs, depending on whether you want to apply the profile to the front physical ports ("Ether alarming") or packet over SDH ("POS alarming"). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.
     Figure 21-4 shows the alarm profiles for an eight-port STM-1 card. CTC shows "Force all ports to Profile: Inherited."

Figure 21-4: Port Alarm Profile for an OC3 IR/STM1 SH 1310-8 Card



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

3. To apply profiles on a port basis:
    1. In card view, click the port row in the Profile column.
    2. Choose the new profile from the drop-down list.
    3. Click Apply.
4. To apply profiles to all ports on a card:
    1. In card view, click the **Force all ports to profile** drop-down arrow at the bottom of the window.
    2. Choose the new profile from the drop-down list.
    3. Click **Force** (still need to "Apply").
    4. Click **Apply**.
       In node view, the Port Level Profiles column indicates port-level profiles with a notation such as "exist (1)" (Figure 18-6).
5. To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.
6. Return to your originating procedure (NTP).

DLP-D427 Delete Alarm Severity Profiles

Purpose	This task deletes a custom or default alarm severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. 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.

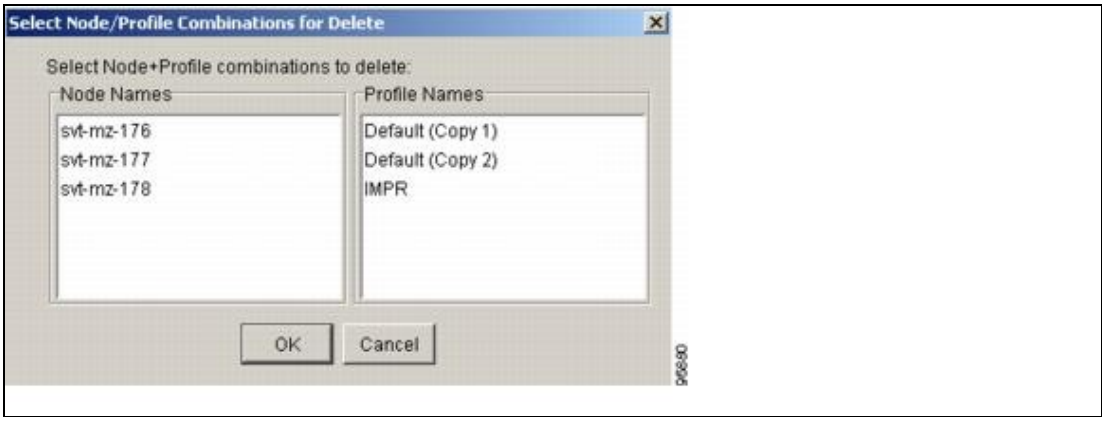
Figure 21-4: Port Alarm Profile for an OC3 IR/STM1 SH 1310-8 Card

- From card view, if the card is an FC_MR-4, E-Series Ethernet, G-Series Ethernet, STM-N, or electrical (DS3i-N-12, E-1, E1-42, or E-3) 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 Profile Editor** tabs or the **Provisioning > POS Alarming > Alarm Profile Editor** tabs, depending on whether you want to apply the profile to the front physical ports ("Ether alarming") or packet over SDH ("POS alarming"). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide.*

2. Click the profile you are deleting to select it.
3. Click **Delete**.

   The Select Node/Profile Combination for Delete dialog box appears (Figure 21-5).

Figure 21-5: 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 8.

4. 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.
5. Click the profile name(s) you want to delete in the Profile Names list.
6. Click OK.
7. 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 Profiles window unless you remove it using the following step.
8. 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, this warning appears if Node A has only Profile 1 stored and the user tries to delete both Profile 1 and Profile 2 from Node A. 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.

9. Return to your originating procedure (NTP).

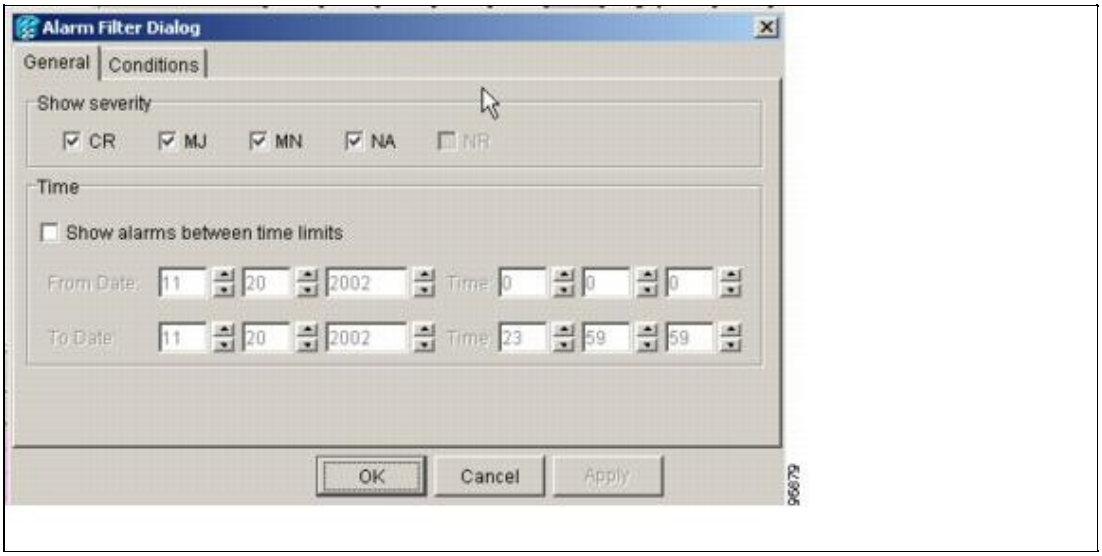
DLP-D428 Modify Alarm, Condition, and History Filtering Parameters

Purpose	This task changes alarm and condition reporting in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-D225 Enable Alarm Filtering DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. At node, network, or card view, click the Alarms, **Conditions**, or **History** tab.
2. Click the **Filter** button at the lower-left of the bottom toolbar.

   The filter dialog box appears, displaying the General tab. Figure 21-6 shows the Alarm Filter dialog box; the Conditions and History tabs have similar dialog boxes.

Figure 21-6: Alarm Filter Dialog Box General Tab



   In the General tab Show Severity area, 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.

3. In the Show Severity area, click the check boxes for the severities (CR, MJ, MN, or Not Alarmed [NA]) that 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.
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.

5. Click the filter dialog box **Conditions** tab (Figure 21-7).

Figure 21-7: Alarm Filter Dialog Box Conditions Tab

Output/110421.jpg

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.

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

Alarm and condition filtering parameters are enforced when alarm filtering is enabled (see the "DLP-D225 Enable Alarm Filtering" task), and are not enforced when alarm filtering is disabled (see the "DLP-D227 Disable Alarm Filtering" task).

7. Return to your originating procedure (NTP).

DLP-D430 Suppress Alarm Reporting

Purpose	This task suppresses the reporting of ONS 15454 SDH alarms at the node, card, or port level.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Caution! If multiple CTC 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 a separate Alarms Suppressed by User Command (AS-CMD) alarm.

1. From node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
2. To suppress alarms for the entire node:
    1. Check the **Suppress Alarms** check box.
    2. 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; this alarm will

show System 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.

3. To suppress alarms for individual cards:
    1. Locate the card row (using the Location column for the slot number or the Eqpt Type column for the equipment name).
    2. Check the **Suppress Alarms** column check box on that row (Figure 18-5).

        Alarms that directly apply to this card change appearance as described in Step 2. For example, if you suppressed raised alarms for an STM-3 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 STM-3 card, the AS-CMD object will be SLOT-16.
    3. Click **Apply**.
4. To suppress alarms for individual card ports, double-click the card in node view.
5. 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, STM-N, or electrical card (DS3i-N-12, E-1, E1-42, or E-3), click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
    - If the card is an ML-Series Ethernet card, click the**Provisioning > Ether Alarming > Alarm Behavior** tabs or the **Provisioning > POS Alarming > Alarm Behavior** tabs, depending on whether you want to apply the profile to the front physical ports ("Ether alarming") or packet over SDH ("POS alarming"). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide.*
6. Check the **Suppress Alarms column** check box for the port row where you want to suppress alarms (Figure 21-4).
7. Click **Apply**.

    Alarms that apply directly to this port 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 appears in either alarm window. For example, if you suppressed alarms for Port 1 on the Slot 16 STM-3 card, the alarm object will be FAC-16-1.
8. Return to your originating procedure (NTP).

DLP-D431 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-D430 Suppress Alarm Reporting DLP-D60 Log into CTC
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.

1. To discontinue alarm suppression for the entire node:
    1. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
    2. 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.

2. To discontinue alarm suppression for individual cards:
    1. In the node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
    2. Locate the card that was suppressed in the slot list.
    3. Uncheck the Suppress Alarms column check box for that slot.
    4. 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.
3. To discontinue alarm suppression for ports, click the following tabs:
    - If the card is an FC_MR-4, E-Series Ethernet, G-Series Ethernet, STM-N, or electrical card (DS3i-N-12, E1-42, or E-3), click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
    - If the card is an ML-Series Ethernet card, click the **Provisioning > Ether Alarming > Alarm Behavior** tabs or the **Provisioning > POS Alarming > Alarm Behavior** tabs, depending on whether you want to apply the profile to the front physical ports ("Ether alarming") or packet over SDH ("POS alarming"). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide.*
4. Uncheck the **Suppress Alarms** check box for the port(s) you no longer want to suppress.
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.
6. Return to your originating procedure (NTP).

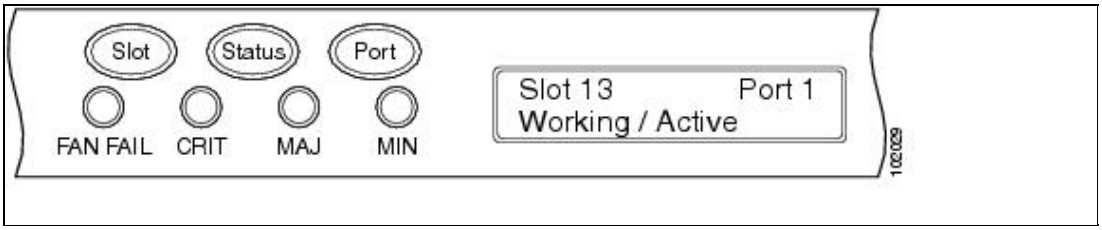
DLP-D432 View Port Status on the LCD

Purpose	This task allows you to view STM-N port status without using CTC. The LCD shows the working/protection provisioning status and the active/standby line status for ports in 1+1 and multiplex section-shared protection ring (MS-SPRing) configurations. For unprotected and subnetwork connection protection (SNCP) ports, the LCD always shows "Working/Active."
Tools/Equipment	None
Prerequisite Procedures	NTP-D16 Install STM-N Cards and Connectors
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

1. Press the **Slot** button on the LCD panel until the desired slot appears on the LCD.
2. Press the **Port** button until the desired port appears on the LCD.
3. Press the **Status** button. After approximately 10 seconds, the LCD will indicate if the port is in working or protect mode and is active or standby.

   Figure 21 shows an example of port status on the LCD panel.

Figure 21-8: Port Status on the LCD Panel



Note: A blank LCD occurs when a fuse on the alarm interface panel (AIP) is blown. If this occurs, contact the Cisco Technical Assistance Center (TAC). See the Obtaining Documentation and Submitting a Service Request for more information.

4. Return to your originating procedure (NTP).

DLP-D433 Run the CTC Installation Wizard for Windows

Purpose	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, Java Runtime Environment (JRE) 5.0, and the CTC Java Archive (JAR) files. JRE 5.0 is required to run Software Release 8.5. Preinstalling the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TCC2/TCC2P card the first time you log in.
Tools/Equipment	Cisco ONS 15454 SDH Release 8.5 software CD
Prerequisite Procedures	None
Required/As Needed	This task is required if any one of the following is true: • JRE 5.0 is not installed. • CTC online user manuals are not installed and are needed. • CTC JAR files are not installed and are needed.
Onsite/Remote	Onsite or remote
Security Level	None

Note: If you will log into nodes running CTC software earlier than R4.6, uninstall JRE 1.4.2 or 5.0 and reinstall JRE 1.3.1_2. To run Software R8.5, uninstall JRE 1.3.1_2 and reinstall JRE 1.4.2 or 5.0. Software R8.5 supports JRE 1.4.2 or JRE 5.0; JRE 1.4.2 is provided on the software CD.

Note: JRE 1.4.2 requires Netscape 7.x or Internet Explorer 6.x.

1. Verify that your computer has the following:
   - Processor-Pentium III, 700 Mhz or faster
   - RAM-384 MB recommended, 512 MB optimum
     Note: Processor and RAM requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM.
   - Hard drive-20 GB hard drive recommended with at least 50 MB of space available
   - Operating system-Windows 98 (1st and 2nd editions), Windows NT 4.0 (with Service Pack 6a), Windows 2000 (with Service Pack 3), Windows XP (with Service Pack 1) or Windows Vista. If your operating system is Windows NT 4.0 go to Step 2. If your operating system is Windows Vista go to Step 3. For all other case go to Step 4.
2. Verify that Service Pack 6a or later is installed. From Windows Start menu, choose **Programs >**

Administrative Tools > Windows NT Diagnostics and check the service pack on the Version tab of the Windows NT Diagnostics dialog box. If Service Pack 6a or later is not installed, do not continue. Install Service Pack 6a following the computer upgrade procedures for your site. Go to Step 4.

3. Complete DLP-D481 Configuring Windows Vista to Support CTC. Go to Step 4.
4. Insert the Cisco ONS 15454 SDH Release 8.5 software CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to the CD directory and double-click **setup.exe**.

   The Cisco Transport Controller Installation wizard displays the components that will be installed on your computer:
   - Java Runtime Environment 5.0
   - Acrobat Reader 6.0.1
   - Online User Manuals
   - CTC JAR files

   Note: JRE 5.0 is required to run Release 8.5. Preinstalling the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TCC2/TCC2P card the first time you log in.
5. Click **Next**.
6. Complete one of the following:
   - Click **Typical** to install both the Java Runtime Environment and the online user manuals.
   - Click **Custom** if you want to install either the JRE or the online user manuals.
7. Click **Next**.
8. Complete the following, as applicable:
   - If you selected Typical in Step 6, skip this step and proceed to Step 9.
   - If you selected Custom, select the CTC component that you want to install and click **Next**.
     - ◊ If you selected Online User Manuals, continue with Step 9.
     - ◊ If you did not select Online User Manuals, continue with Step 11.
9. The directory where the installation wizard will install the CTC online user manuals appears. The default is C:\Program Files\Cisco\CTC\Documentation.
   - If you want to change the CTC online user manuals directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.
   - If you do not want to change the directory, skip this step.
10. Click **Next**.
11. Review the components that will be installed. If you want to change your selections:
    - If you selected Typical in Step 6, click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Steps 7 through 10.
    - If you selected Custom in Step 6, click **Back** once or twice (depending on the components selected) until the component selection page appears. Repeat Steps 8 through 10.
12. Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 6 and need to install a JRE, continue with Step 14.
13. To install the JRE, complete the following:

    1. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:
       - **I accept the terms of the license agreement**-Accepts the license agreement. Continue with SubStep 2.
       - **I do not accept the terms of the license agreement**-Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 14.

       Note: If JRE 1.4.2 is already installed on your computer, the License Agreement page does not appear. You must click Next and then choose Modify to change the JRE installation or Remove to uninstall the JRE. If you choose Modify and click Next, continue with SubStep 5. If you choose Remove and click Next, continue with SubStep 9.

14. Click **Next**.
15. Choose one of the following:
    - ♦ Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
    - ♦ Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.
16. Click **Next**.
17. If you selected Typical, continue with SubStep 9. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:
    - ♦ Java 2 Runtime Environment-(Default) Installs JRE 1.4.2 with support for European languages.
    - ♦ Support for Additional Languages-Adds support for non-European languages.
    - ♦ Additional Font and Media Support-Adds Lucida fonts, Java Sound, and color management capabilities.

    The drop-down list options for each program feature include:
    - ◊ This feature will be installed on the local hard drive-Installs the selected feature.
    - ◊ This feature and all subfeatures will be installed on the local hard drive-Installs the selected feature and all subfeatures.
    - ◊ Don't install this feature now-Does not install the feature (not an option for Java 2 Runtime Environment).

    To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK**.
18. Click **Next**.
19. In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

    Note: Setting the JRE as the default for these browsers might cause problems with these browsers.
20. Click **Next**.
21. Click **Finish**.

    Note: If you are uninstalling the JRE, click **Remove**.

14. In the Cisco Transport Controller Installation wizard, click **Next**. The online user manuals install.
15. Click **Finish**.
16. Return to your originating procedure (NTP).

DLP-D434 Run the CTC Installation Wizard for UNIX

Purpose	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, JRE 1.4.2, and the CTC JAR files. JRE 1.4.2 or 5.0 is required to run CTC Software R8.5. Preinstalling the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TCC2/TCC2P card the first time you login.
Tools/Equipment	Cisco ONS 15454 SDH Release 8.5 software CD
Prerequisite Procedures	None
Required/As Needed	Required if any of the following are true: • JRE 1.4.2 or JRE 5.0 is not installed. • CTC online user manuals are not installed and are needed. • CTC JAR files are not installed and are needed.

Onsite/Remote	Onsite or remote
Security Level	None

Note: If you will log into nodes running CTC software earlier than R4.6, uninstall JRE 1.4.2 or 4.0 and reinstall JRE 1.3.1_2. To run Software R8.5, uninstall JRE 1.3.1_2 and reinstall JRE 1.4.2 or 5.0. Software R8.5 supports JRE 5.0; JRE 1.4.2 is provided on the software CD.

1. Verify that your computer has the following:
   - ♦ RAM-384 MB recommended, 512 MB optimum
   - ♦ Hard drive-20 GB hard drive recommended with at least 50 MB of space available
   - ♦ Operating System-Solaris 8 or 9

   Note: These requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM.
2. Change the directory; type:

   `cd /cdrom/cdrom0/`

3. From the techdoc454 CD directory, type:

   `./setup.bat`

   The Cisco Transport Controller Installation wizard displays the components that will be installed on your computer:
   - · JRE 5.0
   - · Acrobat Reader 6.0.1
   - · Online User Manuals
   - · CTC JAR files
4. Click **Next**.
5. Complete one of the following:
   - · Click **Typical** to install both the Java Runtime Environment and online user manuals. If you already have JRE 5.0 installed on your computer or do not want to install JRE 5.0, choose **Custom**.
   - · Click **Custom** if you want to install either the JRE or the online user manuals.
6. Click **Next**.
7. Complete the following, as applicable:
   - · If you selected Typical in Step 5, continue with Step 8.
   - · If you selected Custom, choose the CTC component that you want to install and click **Next**.
     - ♦ If you selected Online User Manuals, continue with Step 8.
     - ♦ If not, continue with Step 10.
8. The directory where the installation wizard will install CTC online user manuals appears. The default is /usr/doc/ctc.
   - · If you want to change the CTC online user manuals directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.
   - · If you do not want to change the CTC online user manuals directory, skip this step.
9. Click **Next**.
10. Review the components that will be installed. To change the components, complete one of the following:
    - · If you selected Typical in Step 5, click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Steps 6 through 9.
    - · If you selected Custom in Step 5, click **Back** once or twice (depending on the components selected) until the component selection page appears. Repeat Steps 7 through 9.

11. Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 6 and need to instal l a JRE, continue with Step 13.
12. To install the JRE, complete the following:
    1. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:

       - **I accept the terms of the license agreement**-Accepts the license agreement. Continue with SubStep 2.
       - **I do not accept the terms of the license agreement**-Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 13.
         Note: If JRE 5.0 is already installed on your computer, the License Agreement page does not appear. You must click Next and then choose Modify to change the JRE installation or Remove to uninstall the JRE. If you choose Modify and click Next, continue with SubStep 5. If you choose Remove and click Next, continue with SubStep 9.

    2. Click **Next**.
    3. Choose one of the following:

       - Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
       - Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

    4. Click **Next**.
    5. If you selected Typical, continue with SubStep 9. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

       - Java 2 Runtime Environment-(Default) Installs JRE 5.0 with support for European languages.
       - Support for Additional Languages-Adds support for non-European languages.
       - Additional Font and Media Support-Adds Lucida fonts, Java Sound, and color management capabilities.

       The drop-down list options for each program feature include:
       - This feature will be installed on the local hard drive-Installs the selected feature.
       - This feature and all subfeatures will be installed on the local hard drive-Installs the selected feature and all subfeatures.
       - Don't install this feature now-Does not install the feature (not an option for Java 2 Runtime Environment).

       To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK**.
    6. Click **Next**.
    7. In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

       Note: Setting the JRE version as the default for these browsers might cause problems with these browsers.
    8. Click **Next**.

9. Click **Finish**.
   Note: If you are uninstalling the JRE, click **Remove**.
13. In the Cisco Transport Controller Installation wizard, click **Next**. The Online User Manuals installs.
14. Click **Finish**.
    Note: Be sure to record the names of the directories you choose for JRE and the online user manuals.
15. Return to your originating procedure (NTP).

DLP-D435 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-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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.

1. From the Edit menu, choose **Preferences > Map** and check the **Use Default Map** check box.
2. Change the left and right Latitude and Longitude for the map.
3. Click the **Provisioning > Defaults** tabs.
4. In the Defaults Selector area, choose **CTC** and then **Network**.
5. 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).
6. Click **Apply**. The new network map appears.
7. Click **OK**.
8. If the ONS 15454 SDH icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the ONS 15454 SDH icons are visible. (You can also choose **Fit Graph to Window**.)
9. If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.
10. If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 SDH icons appear at the magnification you want.
11. Return to your originating procedure (NTP).

DLP-D436 Delete Ethernet RMON Alarm Thresholds

Purpose	This task deletes remote monitoring (RMON) threshold crossing alarms for Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-D441 Create Ethernet RMON Alarm Thresholds DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: The ONS 15454 SDH ML-Series cards use the Cisco IOS command line interface (CLI) for managing RMON.

1. Double-click the Ethernet card where you want to delete the RMON alarm thresholds.
2. In card view, click the **Provisioning > RMON Thresholds** tabs.
3. Click the RMON alarm threshold you want to delete.
4. Click **Delete**. The Delete Threshold dialog box appears.
5. Click **Yes** to delete that threshold.
6. Return to your originating procedure (NTP).

DLP-D437 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 SDH and sets the user security level that can clear node performance monitoring data.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Note: After TCC reset, backplane LAN access gets enabled even if you have set the Access type to No LAN Access.

  - ◊ **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.

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) or 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.

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.
5. In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: **PROVISIONING** or **SUPERUSER**.
6. Select the Enable Craft Port check box to turn on the shelf controller serial ports.
7. Select the element management system (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**-(Default) Uses Port 57790 to connect to ONS 15454s on the same side of the firewall or if no firewall is used. 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.
8. In the SNMP Access area, set the Simple Network Management Protocol (SNMP) access state to Non-Secure or Disabled (disables SNMP access).
9. Click **Apply**.
10. Return to your originating procedure (NTP).

DLP-D438 Change Port Settings for the FC_MR-4 Card

Purpose	This task changes the port settings for FC_MR-4 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, double-click the FC_MR-4 card where you want to change the port settings.
2. Click the **Provisioning > Port** tabs.
3. Modify any of the settings described in Table 21-1.

Table 21-1: FC_MR-4 Card Port Settings

Parameter	Description	Options
#	(Display only) Displays the port number.	1 through 4
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-D314 Assign a Name to a Port" task.
State	Places port in service, out of service, or out of service-maintenance.	• IS • OOS • OOS_MT
Port Rate	Selects the Fibre Channel interface.	

		• 1 Gbps • 2 Gbps
Link Rate	Displays the actual rate of the port.	-
Max GBIC Rate	Displays the maximum Gigabit Interface Converter (GBIC) rate. Cisco supports two GBICs for the FC_MR-4 card (ONS-GX-2FC-SML and ONS-GX-2FC-MMI). If used with another GBIC, "Contact GBIC vendor" appears in this field.	-
Enable Link Recovery	Enables or disables link recovery if a local port is inoperable. If enabled, a link reset occurs when there is a loss of transport from a cross-connect switch, a protection switch, or an upgrade.	-

4. Click **Apply**.
5. Return to your originating procedure (NTP).

DLP-D441 Create Ethernet RMON Alarm Thresholds

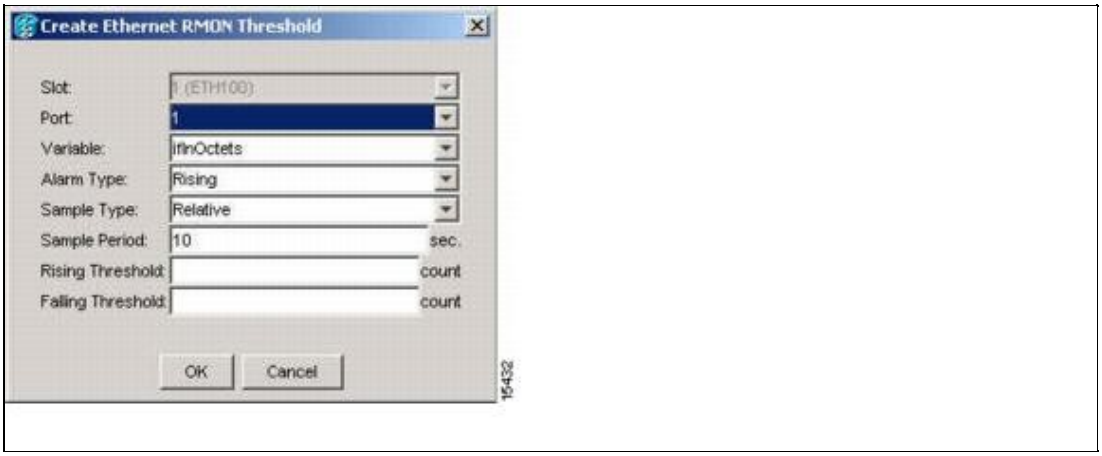
Purpose	This task sets up RMON to allow network management systems (NMSs) to monitor Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-D24 Verify Card Installation
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: The ONS 15454 SDH ML-Series cards use the Cisco IOS CLI for managing RMON.

1. Complete the [[ONS 15454 SDH Procedure Guide R8.5.1 -- DLPs D1 to D99#"DLP-D60 Log into CTC" task on page 17-44 at the node where you want to set up remote monitoring.
2. Double-click the Ethernet card where you want to create the RMON alarm thresholds.
3. In card view, click the **Provisioning > RMON Thresholds** tabs.
4. Click **Create**.

   The Create Ether Threshold dialog box appears (Figure 21-9).

Figure 21-9: Creating Ethernet RMON Thresholds



5. From the Slot drop-down list, choose the appropriate Ethernet card.
6. From the Port drop-down list, choose the applicable port on the Ethernet card that you selected.
7. From the Variable drop-down list, choose the variable. See Table 21-2 for a list of the Ethernet threshold variables available in this field.

Table 21-2: 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 only) Number of multicast frames received error free.
ifInBroadcastPkts	(G-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 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 only) Number of multicast frames transmitted error free.
ifOutBroadcastPkts	(G-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 that would 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).
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 signaling sublayer (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 IEEE 802.3 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 IEEE 802.3 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.
etherStatsCollisionFrames	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 IEEE 802.3 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 IEEE 802.3 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.
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.
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.
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.

8. 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.
9. 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.
10. Type in an appropriate number of seconds in the Sample Period field.
11. Type in the appropriate number of occurrences in the Rising Threshold field.

    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 falling threshold of 400 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, the excess collisions trigger an alarm.

12. 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 seconds subsides and creates only 799 collisions in 15 seconds, 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 second 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).

13. Click **OK** to complete the procedure.
14. Return to your originating procedure (NTP).

DLP-D442 Preprovision a Slot

Purpose	This task preprovisions a card slot in CTC before you physically install the card in the ONS 15454 SDH.
Tools/Equipment	None
Prerequisite Procedures	Connect the PC and Log into the GUI
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, right-click the empty slot where you will later install a card.
2. From the Add Card shortcut menu, choose the card type that will be installed. Only cards that can be installed in the slot appear in the Add Card shortcut menu.

   Note: When you preprovision a slot, the card appears purple in the CTC shelf graphic, rather than white when a card is installed in the slot. NP (not present) on the card graphic indicates that the card is not physically installed.
3. Return to your originating procedure (NTP).

DLP-D457 Refresh E-Series and G-Series Ethernet PM Counts

Purpose	This task changes the window view to display specified E-Series and G-Series Ethernet PM counts in time intervals depending on the interval option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, double-click the card where you want to view PM counts. The card view appears.
2. Click the **Performance > History** tabs.
3. From the Interval drop-down list, choose one of the following:
   - 1 min
   - 15 min
   - 1 hour
   - 1 day
4. Click **Refresh**. Performance monitoring information appears in the interval selected synchronized with the time of day.
5. View the Prev column to find PM counts for the latest selected interval.

   Each monitored performance parameter has corresponding threshold values for the latest time period. If the value of the counter exceeds the threshold value for a particular selected interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.
6. View the Prev-*n* columns to find PM counts for the previous intervals.

If a complete count over the selected interval is not possible, the value appears with a yellow background. For example, if you selected the 1-day interval, an incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 1-day interval appears with a white background.

7. Return to your originating procedure (NTP).

DLP-D458 Monitor PM Counts for a Selected Signal

Purpose	This task uses signal-type selections to monitor near-end or far-end PM counts for specific signals on a selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, double-click the card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.

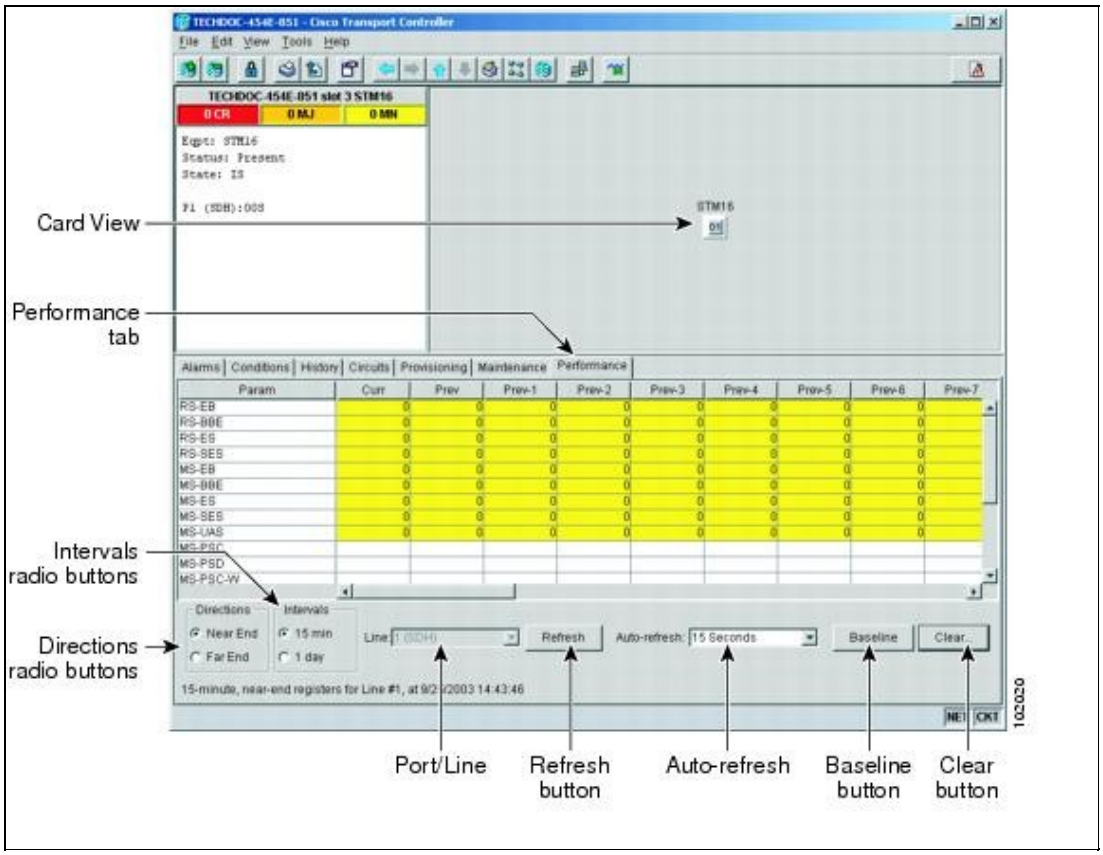
   Different port and signal-type drop-down lists appear depending on the card type and the circuit type. The appropriate signal types (DS3i, E1, E3, STM-N line, and VC4) appear based on the selected card. For example, the STM16 LH AS 1550 card lists the line and VC4 PM parameters as signal types, which enables you to select both the line and the VC4 within the specified line.

3. In the signal type drop-down lists, click one of the following options:

   · Port: *n* (card port number)
   · Line: *n* (STM line number)
   · VC4: *n* (VC path number within the STM line)

   Figure 21-10 shows the Line drop-down list in the Performance window for an STM-16 card.

Figure 21-10: Line Drop-down List for an STM-16 Card



4. Click **Refresh**. All PM counts recorded by the near-end or far-end node for the specified outgoing signal type on the selected card and port appear. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual.*
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 SDH Reference Manual*.
6. Return to your originating procedure (NTP).

DLP-D459 Clear Selected PM Counts

Purpose	This task uses the Clear button to clear specified PM counts depending on the option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution! Pressing the Clear button can mask problems if used incorrectly. This button is commonly used for testing purposes. After pressing this button, the current bin is marked invalid. Also note that the unavailable seconds (UAS) state is not cleared if you were counting UAS; therefore, this count could be unreliable when UAS is no longer incrementing.

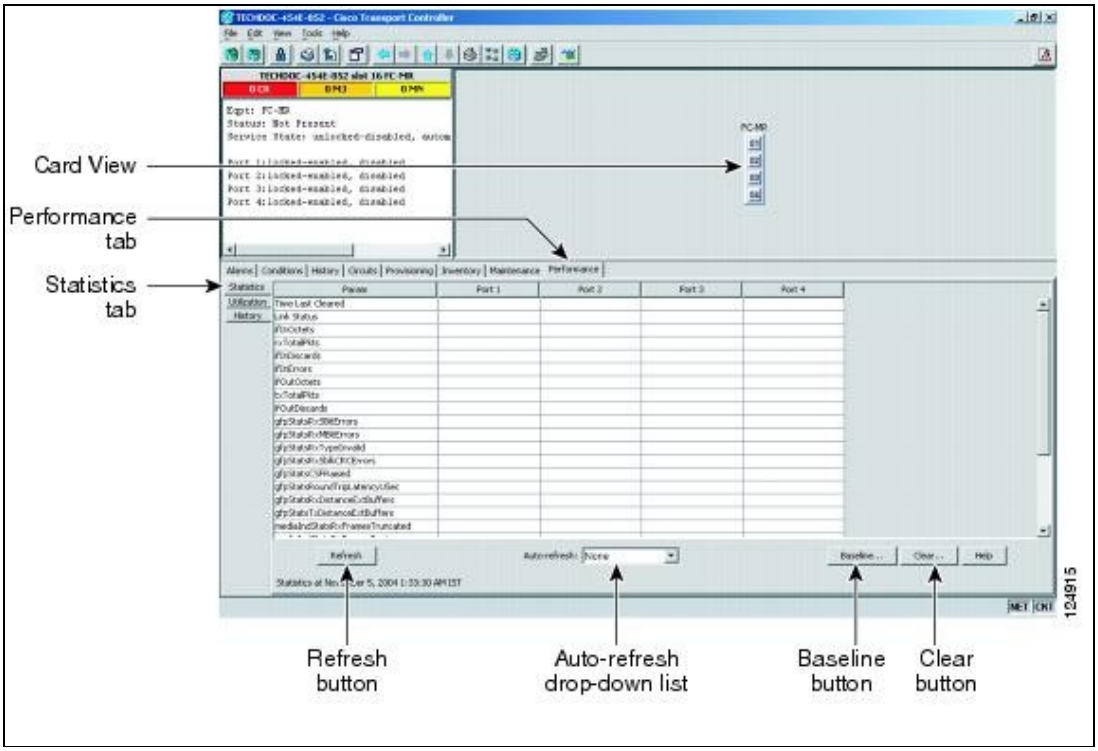
1. In node view, double-click the card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.
3. Click **Clear**.
4. In the Clear Statistics dialog box, choose one of the following options:
    - **Displayed statistics**-Clearing the displayed statistics erases from the card and the window all PM counts associated with the current combination of statistics on the selected port. This means that the selected time interval, direction, and signal type counts are erased from the card and the window.
    - **All statistics for port** *x*-Clearing all statistics for port *x* erases from the card and the window all PM counts associated with all combinations of the statistics on the selected port. This means that all time intervals, directions, and signal type counts are erased from the card and the window.
    - **All statistics for card**-Clearing all statistics for a card erases from the card and the window all PM counts for all ports.
5. Choose **OK** to clear the selected statistics.
6. Verify that the selected PM counts have been cleared.
7. Return to your originating procedure (NTP).

DLP-D460 View FC_MR-4 Statistics PM Parameters

Purpose	This task enables you to view current statistical PM counts on an FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.
2. Click the **Performance > Statistics** tabs (Figure 21-11).

Figure 21-11: FC_MR-4 Statistics in the Card View Performance Window



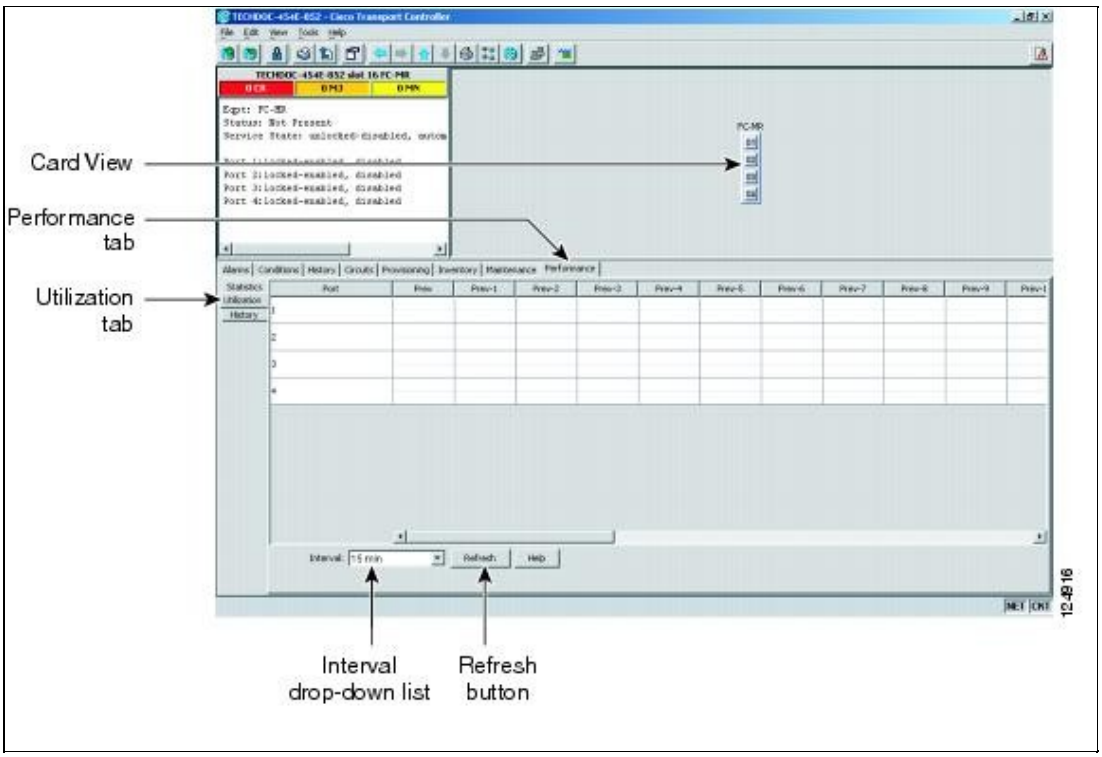
3. Click **Refresh**. Performance monitoring statistics for each port on the card appear.
4. View the PM parameter names that appear in the Param column. The current PM parameter values appear in the port number columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual*.
5. Return to your originating procedure (NTP).

DLP-D461 View FC_MR-4 Utilization PM Parameters

Purpose	This task enables you to view line utilization PM counts on an FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.
2. Click the **Performance > Utilization** tabs (Figure 21-12).

Figure 21-12: FC_MR-4 Utilization in the Card View Performance Window



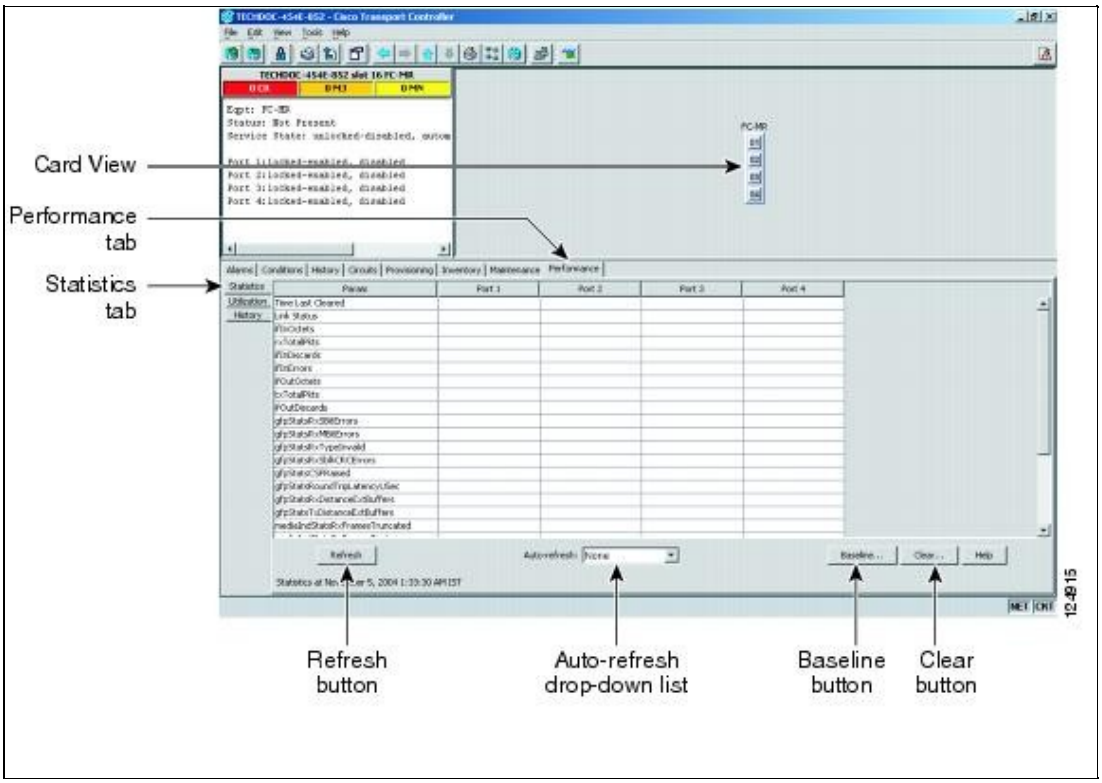
3. Click **Refresh**. Performance monitoring utilization values for each port on the card appear.
4. View the port number column to find the port you want to monitor.
5. The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual*.
6. Return to your originating procedure (NTP).

DLP-D462 View FC_MR-4 History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on an FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.
2. Click the **Performance > History** tabs (Figure 21-13).

Figure 21-13: FC_MR-4 History in the Card View Performance Window



3. Click **Refresh**. Performance monitoring statistics for each port on the card appear.
4. View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual*.
5. Return to your originating procedure (NTP).

DLP-D463 Refresh FC_MR-4 PM Counts at a Different Time Interval

Purpose	This task changes the window view to display specified PM counts in time intervals depending on the interval option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.
3. Click the **Utilization** or the **History** tab.
4. From the Interval drop-down list, choose one of four options:
   - **1 min**-This option displays the specified PM counts in one-minute time intervals.
   - **15 min**-This option displays the specified PM counts in 15-minute time intervals.
   - **1 hour**-This option displays the specified PM counts in one-hour time intervals.
   - **1 day**-This option displays the specified PM counts in one-day (24 hours) time intervals.
5. Click **Refresh**. The PM counts refresh with values based on the selected time interval.
6. Return to your originating procedure (NTP).

Figure 21-13: FC_MR-4 History in the Card View Performance Window

DLP-D465 Create FC_MR-4 RMON Alarm Thresholds

Purpose	This procedure sets up RMON to allow network management systems (NMSs) to monitor FC_MR-4 ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-D24 Verify Card Installation DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, double-click the FC_MR-4 card where you want to create the RMON alarm thresholds.
2. In card view, click the **Provisioning > RMON Thresholds** tabs.
3. Click **Create**. The Create Threshold dialog box appears.
4. From the Slot drop-down list, choose the appropriate FC_MR-4 card.
5. From the Port drop-down list, choose the applicable port on the FC_MR-4 card you selected.
6. From the Variable drop-down list, choose the variable. See Table 21-3 for a list of the FC_MR-4 threshold variables available in this field in line rate mode. See Table 21-4 for a list of the FC_MR-4 threshold variables available in this fields in enhanced mode.

Table 21-3: FC_MR-4 Threshold Variables for Fibre Channel/FICON Line Rate Mode (MIBs)

Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets.
ifInDiscards	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.
ifOutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
txTotalPkts	Total number of transmit packets.
rxTotalPkts	Total number of receive packets.
fibreStatsInvalidOrderedSets	Received ordered sets that are not recognized as part of the defined Fibre Channel control words.
fibreStatsEncodingDispErrors	Received control words that cannot be decoded due to invalid disparity.
fibreStatsRxFramesTooLong	Received oversize Fibre Channel frames > 2148 including cyclic redundancy check (CRC).
fibreStatsRxFramesBadCRC	Received Fibre Channel frames with bad CRC.
fibreStatsRxFrames	Received total Fibre Channel frames.
fibreStatsRxOctets	Received total Fibre Channel data bytes within a frame.
fibreStatsTxFramesBadCRC	Transmitted Fibre Channel frames with bad CRC.
fibreStatsTxFrames	Transmitted total Fibre Channel frames.
fibreStatsTxOctets	Transmitted total Fibre Channel data bytes within a frame.
fibreStatsLinkResets	

	Total number of link resets initiated by FCMR port when link recovery port setting is enabled.
gfpStatsRxSBitErrors	Received generic framing protocol (GFP) frames with single bit errors in the core header (these errors are correctable).
gfpStatsRxMBitErrors	Received GFP frames with multiple bit errors in the core header (these errors are not correctable).
gfpStatsRxTypeInvalid	Received GFP frames with invalid type (these are discarded). For example, receiving GFP frames that contain Ethernet data when Fibre Channel data is expected.
gfpStatsRxSblkCRCErrors	Total number of superblock CRC errors with the receive transparent GFP frame. A transparent GFP frame has multiple superblocks that each contain Fibre Channel data.
gfpStatsCSFRaised	Number of Rx client management frames with Client Signal Fail indication.
mediaIndStatsTxFramesTooLong	Number of packets transmitted that are greater than 1548 bytes.
mediaIndStatsRxFramesTruncated	Total number of frames received that are less than 5 bytes.

Table 21-4: FC_MR-4 Threshold Variables for Fibre Channel/FICON Enhanced Mode (MIBs)

Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets.
ifInDiscards	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.
ifOutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
fcIngressRxDistanceExtBuffers	The maximum number of GFP buffers that are available at the GFP receiver.
fcEgressTxDistanceExtBuffers	The number of GFP buffers that the GFP transmitter is allowed to transmit. Remote GFP receiver tells the GFP transmitter how many buffers it has available.
fcStatsLinkRecoveries	The number of times a link reset was initiated due to a GFP out of frame condition. This is only valid when link recovery is enabled and is not valid when distance extension is enabled.
fcStatsRxCredits	The maximum number of Fibre Channel credits that the Fibre Channel/fiber connectivity (FICON) link partner will allow the FCMR Fibre Channel/FICON transmitter to transmit (that is, the maximum number of frames the link partner can receive).
fcStatsTxCredits	The number of Fibre Channel credits that the FCMR Fibre Channel/ficon transmitter is left with. This is the number of frames that the Fibre Channel/FICON transmitter has available to send. **Note:** The Tx credits increment whenever a credit is received from the link partner, and decrement when a frame is sent.
fcStatsZeroTxCredits	A count that increments when the Fibre Channel/FICON Tx credits go from a nonzero value to zero.
fibreStatsInvalidOrderedSets	Received ordered sets that are not recognized as part of the defined Fibre Channel control words.

fibreStatsEncodingDispErrors	Received control words that cannot be decoded due to invalid disparity.
fibreStatsRxFramesTooLong	Received oversize Fibre Channel frames that are greater than 2148 including CRC.
fibreStatsRxFramesBadCRC	Received Fibre Channel frames with bad CRC.
fibreStatsRxFrames	Received total Fibre Channel frames.
fibreStatsRxOctets	Received total Fibre Channel data bytes within a frame.
fibreStatsTxFramesBadCRC	Transmitted Fibre Channel frames with bad CRC.
fibreStatsTxFrames	Transmitted total Fibre Channel frames.
fibreStatsTxOctets	Transmitted total Fibre Channel data bytes within a frame.
fibreStatsLinkResets	Total number of link resets initiated by FCMR port when link recovery port setting is enabled.
gfpStatsRxSBitErrors	Received GFP frames with single bit errors in the core header (these errors are correctable).
gfpStatsRxMBitErrors	Received GFP frames with multiple bit errors in the core header (these errors are not correctable).
gfpStatsRxTypeInvalid	Received GFP frames with invalid type (these are discarded). For example, receiving GFP frames that contain Ethernet data when Fibre Channel data is expected.
gfpStatsRxSblkCRCErrors	Total number of superblock CRC errors with the receive transparent GFP frame. A transparent GFP frame has multiple superblocks which each contain Fibre Channel data.
8b10bInvalidOrderedSets	Total number of ordered sets not compliant to Gigabit Ethernet/Fibre Channel (GE/FC) standard.
8b10bStatsEncodingDispErrors	Total number of code groups that violate GE/FC disparity errors.

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.
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.
9. Type in an appropriate number of seconds in the Sample Period field.
10. Type in the appropriate number of occurrences in the Rising Threshold field.

    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.

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 seconds subsides and creates only 799 collisions in 15 seconds, 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-second 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).

12. Click **OK** to complete the procedure.
13. Return to your originating procedure (NTP).

DLP-D466 Delete FC_MR-4 RMON Alarm Thresholds

Purpose	This task deletes RMON threshold crossing alarms for FC_MR-4 ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-D465 Create FC_MR-4 RMON Alarm Thresholds DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, double-click the FC_MR-4 card where you want to delete the RMON alarm thresholds.
2. In card view, click the **Provisioning > Line Thresholds** tabs.
3. Click the RMON alarm threshold you want to delete.
4. Click **Delete**. The Delete Threshold dialog box appears.
5. Click **Yes** to delete that threshold.
6. Return to your originating procedure (NTP).

DLP-D468 Create a Two-Fiber MS-SPRing Using the MS-SPRing Wizard

Purpose	This task creates a two-fiber MS-SPRing using the MS-SPRing wizard.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed; required to complete MS-SPRing setup
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. From the View menu, choose **Go to Network View**.
2. Click the **Provisioning > MS-SPRing** tabs.
3. Click **Create MS-SPRing**.
4. In the MS-SPRing Creation dialog box, set the MS-SPRing properties:
    - Ring Type-Choose **two-fiber**.
    - Speed-Choose the MS-SPRing speed: STM-4, STM-16, or STM-64. The speed must match the STM-N speed of the MS-SPRing trunk (span) cards.
      Note: If you are creating an STM-4 MS-SPRing and will eventually upgrade it to STM-16 or STM-64, use the single-port STM-4 cards (OC12 IR/STM4 SH 1310, OC12 IR/STM4 SH 1310, or OC12 IR/STM4 SH 1310). You cannot upgrade an MS-SPRing on a four-port STM-4 (OC12/STM4-4) because STM-16 and STM-64 cards are single-port cards.
    - Ring Name-Assign a ring name. The name can be from 1 to 6 characters in length. Any alphanumeric character string is permissible, and upper and lower case letters can be combined. Do not use the character string "All" in either uppercase or lowercase letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another MS-SPRing.

- Reversion time-Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversions can be set to Never.

5. Click **Next**. If the network graphic appears, go to Step 6. If CTC determines that an MS-SPRing cannot be created, for example, not enough optical cards are installed or it finds circuits with SNCP selectors, a "Cannot Create MS-SPRing" message appears. If this occurs, complete the following steps:
    1. Click **OK**.
    2. In the Create MS-SPRing window, click **Excluded Nodes**. Review the information explaining why the MS-SPRing could not be created, then click **OK**.
    3. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.
    4. Complete the NTP-D40 Provision MS-SPRing Nodes, making sure all steps are completed accurately, then start this procedure again.
6. In the network graphic, double-click an MS-SPRing span line. If the span line is DCC connected to other MS-SPRing cards constituting a complete ring, the lines turn blue and the Finish button appears. If the lines do not form a complete ring, double-click span lines until a complete ring is formed. When the ring is DCC connected, go to the next step.
7. Click **Finish**. If the MS-SPRing window appears with the MS-SPRing you created, go to Step 8. If a "Cannot Create MS-SPRing" or "Error While Creating MS-SPRing" message appears:
    1. Click **OK**.
    2. In the Create MS-SPRing window, click **Excluded Nodes.** Review the information explaining why the MS-SPRing could not be created, then click **OK**.
    3. Depending on the problem, click **Back** to start over or click **Cancel t**o cancel the operation.
    4. Complete the NTP-D40 Provision MS-SPRing Nodes, making sure all steps are completed accurately, then start this procedure again.

    Note: Some or all of the following alarms might briefly appear during MS-SPRing setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and MSSP-OSYNC.
8. Verify the following:
    - On the network view graphic, a green span line appears between all MS-SPRing nodes.
    - All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and MSSP-OSYNC alarms are cleared. See the *Cisco ONS 15454 SDH Troubleshooting Guide* for alarm troubleshooting.

    Note: The numbers in parentheses after the node name are the MS-SPRing node IDs assigned by CTC. Every ONS 15454 SDH in an MS-SPRing is given a unique node ID, 0 through 31. To change it, complete the "DLP-D24 Change an MS-SPRing Node ID" task.
9. Return to your originating procedure (NTP).

DLP-D469 Create a Two-Fiber MS-SPRing Manually

Purpose	This task creates a two-fiber MS-SPRing at each MS-SPRing-provisioned node without using the MS-SPRing wizard.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > Ring** tabs.
2. Click **Create**.
3. In the Suggestion dialog box, click **OK**.

4. In the Create MS-SPRing dialog box, set the MS-SPRing properties:
   - Ring Type-Choose **two-fiber**.
   - Ring Name-Assign a ring name. You must use the same ring name for each node in the MS-SPRing. Any alphanumeric character string is permissible, and uppercase and lowercase letters can be combined. Do not use the character string "All" in either upper or lower case letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another MS-SPRing.
   - Node ID-Choose a Node ID from the drop-down list (0 through 31). The Node ID identifies the node to the MS-SPRing. Nodes in the same MS-SPRing must have unique Node IDs.
   - Reversion time-Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in an MS-SPRing must have the same reversion time setting.
   - West Line-Assign the west MS-SPRing port for the node from the drop-down list. The east and west ports must match the fiber connections and DCC terminations set up in the NTP-D40 Provision MS-SPRing Nodes.
   - East Line-Assign the east MS-SPRing port for the node from the drop-down list.
5. Click **OK**.

   Note: Some or all of the following alarms will appear until all the MS-SPRing nodes are provisioned: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and MS-SPRINGOSYNC. The alarms clear after you configure all of the nodes in the MS-SPRing.
6. From the View menu, choose **Go to Other Node**.
7. In the Select Node dialog box, choose the next node that you want to add to the MS-SPRing.
8. Repeat Steps 1 through 7 at each node that you want to add to the MS-SPRing. When all nodes have been added, continue with Step 9.
9. From the View menu, choose **Go to Network View**. After 10 to 15 seconds, verify the following:
   - A green span line appears between all MS-SPRing nodes.
   - All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and MS-SPRINGOSYNC alarms are cleared.
10. Return to your originating procedure (NTP).

DLP-D470 Manually Route an SNCP Circuit for a Topology Upgrade

Purpose	This task creates a manually routed USPR circuit during a conversion from an unprotected point-to-point or linear ADM system to a SNCP.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC NTP-D351 Convert a Point-to-Point or Linear ADM to an SNCP Automatically
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In the Circuit Routing Preferences area of the Unprotected to SNCP page, uncheck **Route Automatically**.
2. Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.
3. Click **Finish**.
4. Return to your originating procedure (NTP).

DLP-D471 Automatically Route an SNCP Circuit for a Topology Upgrade

Purpose	This task creates an automatically routed SNCP circuit during a conversion from an unprotected point-to-point or linear ADM system to an SNCP.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC NTP-D351 Convert a Point-to-Point or Linear ADM to an SNCP Automatically
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: This task requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 SDH Reference Manual*.

1. In the Circuit Routing Preferences area of the Unprotected to SNCP page, check **Route Automatically**.
2. Check the **Review Route Before Creation** check box if you want to review and edit the circuit route before the circuit is created.
3. Choose one of the following:
   - **Nodal Diversity Required**-Ensures that the primary and alternate paths within SNCP portions of the complete circuit path are nodally diverse.
   - **Nodal Diversity Desired**-Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the SNCP portion of the complete circuit path.
   - **Link Diversity Only**-Specifies that only fiber-diverse primary and alternate paths for SNCP portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.
4. If you selected Review Route Before Creation in Step 2, complete the following substeps. If not, continue with Step 5.
   1. Click **Next**.
   2. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.
   3. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the NTP-D134 Create a Manually Routed Low-Order Tunnel.
5. Click **Finish**.
6. Return to your originating procedure (NTP).

DLP-D472 Install the CTC Launcher Application from a Release 8.5 Software CD

Purpose	This task installs the CTC Launcher from a Release 8.5 software CD.
Tools/Equipment	None
Prerequisite Procedures	NTP-D278 Set Up Computer for CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

1. Insert the Cisco ONS 15454 or Cisco ONS 15454 SDH or Cisco ONS 15310-CL or Cisco ONS 15310-MA Software Release 8.5 CD into your CD drive.
2. Navigate to the CtcLauncher directory.
3. Save the StartCTC.exe file to a local hard drive.
4. Return to your originating procedure (NTP).

DLP-D473 Install the CTC Launcher Application from a Release 8.5 Node

Purpose	This task installs the CTC Launcher from an ONS 15454 SDH node running Software R8.5.
Tools/Equipment	None
Prerequisite Procedures	NTP-D278 Set Up Computer for CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

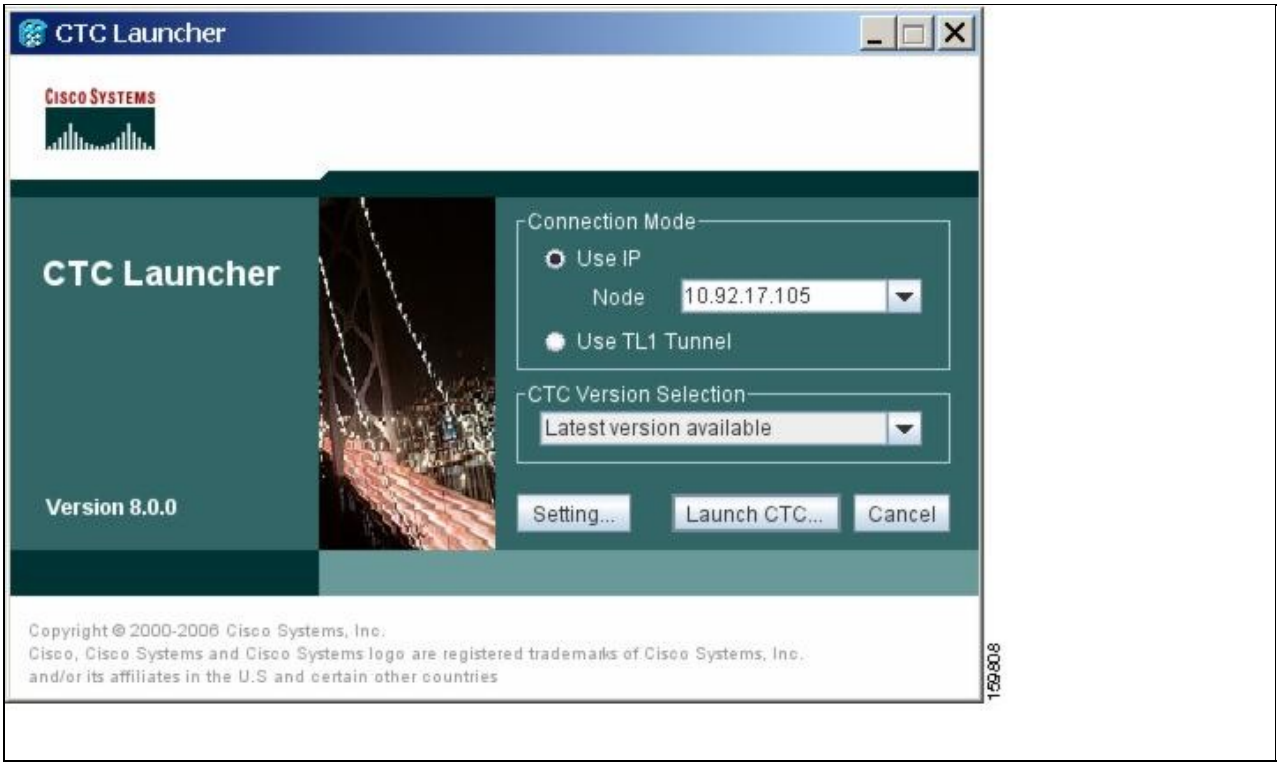
1. Using a web browser, go to the following address, where *node-name* is the DNS name of a node you are going to access:
   http://*node-name*/fs/StartCTC.exe
   The browser File Download dialog box appears.
2. Click **Save**
3. Navigate to the location where you want to save the StartCTC.exe file to a local hard drive.
4. Click **Save**.
5. Return to your originating procedure (NTP).

DLP-D474 Connect to ONS Nodes Using the CTC Launcher

Purpose	This task starts the CTC Launcher from an ONS node.
Tools/Equipment	None
Prerequisite Procedures	NTP-D278 Set Up Computer for CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

1. Start the CTC Launcher:
   - Windows: navigate to the directory containing the StartCTC.exe file and double-click it. (You can also use the Windows Start menu Run command.)
   - Solaris: assuming the StartCTC.exe file is accessible from the current shellpath, navigate to the directory containing the CtcLauncher.jar file and type:
     % java -jar StartCTC.exe
2. In the CTC Launcher dialog box, choose **Use IP**.
   Figure 21-14 shows the CTC Launcher window.

Figure 21-14: CTC Launcher Window



3. In the Login Node box, enter the ONS NE node name or IP address. (If the address was entered previously, you can choose it from the drop-down menu.)
4. Select the CTC version you want to launch from the following choices in the drop-down menu:

   · Same version as the login node: Select if you want to launch the same CTC version as the login node version, even if more recent versions of CTC are available in the cache.
   · Latest version available: Select if you want to launch the latest CTC version available. If the cache has a newer CTC version than the login node, that CTC version will be used. Otherwise the same CTC version as the login node will be used.
   · Version x.xx: Select if you want to launch a specific CTC version.

   Note: Cisco recommends that you always use the "Same version as the login node" unless the use of newer CTC versions is desired (for example, when CTC must manage a network containing mixed version NEs).
5. Click **Launch CTC**. After the connection is made, the CTC Login dialog box appears.
6. Log into the ONS node.

   Note: Because each CTC version requires particular JRE versions, the CTC Launcher will prompt the user for the location of a suitable JRE whenever a new CTC version is launched for the first time using a file chooser dialog (if a suitable JRE version is not known by the launcher yet). That JRE information is then saved in the user's preferences file. From the selection dialog, select any appropriate JRE directory. After the JRE version is selected, the CTC will be launched. The required jar files will be downloaded into the new cache if they are missing. The CTC Login window will appear after a few seconds.
7. Return to your originating procedure (NTP).

Figure 21-14: CTC Launcher Window

DLP-D475 Create a TL1 Tunnel Using the CTC Launcher

Purpose	This task creates a TL1 tunnel using the CTC Launcher, and the tunnel transports the TCP traffic to and from ONS ENEs through the OSI-based GNE.
Tools/Equipment	None
Prerequisite Procedures	NTP-D278 Set Up Computer for CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

1. Double-click the StartCTC.exe file.
2. Click **Use TL1 Tunnel**.
3. In the Open CTC TL1 Tunnel dialog box, enter the following:
    - Far End TID-Enter the TID of the ONS ENE at the far end of the tunnel. The TID is the name entered in the Node Name field on the node view **Provisioning > General** tab.
    - Host Name/IP Address-Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS node through an OSI DCC network. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the end network elements (ENEs).
    - Choose a port option:
        - Use Default TL1 Port-Choose this option if you want to use the default TL1 port 3081 and 3082.
        - Use Other TL1 Port-Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
    - TL1 Encoding Mode-Choose the TL1 encoding:
        - LV + Binary Payload- TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient encoding mode. However, you must verify that the GNE supports LV + Binary Payload encoding.
        - LV + Base64 Payload- TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
        - Raw-TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
    - GNE Login Required-Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
    - TID-If the GNE Login Required box is checked, enter the GNE TID.
4. Click **OK**.
5. If the GNE Login Required box is checked, complete the following steps. If not, continue Step 6.
    1. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.
    2. In the PID field, enter the TL1 user password.
    3. Click **OK**.
6. When the CTC Login dialog box appears, complete the CTC login.
7. Return to your originating procedure (NTP).

DLP-D476 Create a TL1 Tunnel Using CTC

Purpose	This task creates a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

1. From the Tools menu, choose **Manage TL1 Tunnels**.
2. In the TL1 Tunnels window, click **Create**.
3. In the Create CTC TL1 Tunnel dialog box, enter the following:
    - Far End TID-Enter the TID of the ONS ENE at the far end of the tunnel. The ENE must be a Cisco ONS NE. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.
    - Host Name/IP Address-Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
    - Choose a port option:
        - Use Default TL1 Port-Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
        - Use Other TL1 Port-Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
    - TL1 Encoding Mode-Choose the TL1 encoding:
        - LV + Binary Payload- TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
        - LV + Base64 Payload- TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
        - Raw-TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
    - GNE Login Required-Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
    - TID-If the GNE Login Required box is checked, enter the GNE TID.
4. Click **OK**.
5. If the GNE Login Required box is checked, complete the following steps. If not, continue Step 6.
    1. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.
    2. In the PID field, enter the TL1 user password.
    3. Click **OK**.
6. After the CTC Login dialog box appears, log into CTC.
7. Return to your originating procedure (NTP).

DLP-D477 View TL1 Tunnel Information

Purpose	This task views a TL1 tunnel created using the CTC Launcher.
Tools/Equipment	None
Prerequisite Procedures	NTP-D278 Set Up Computer for CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

1. Log into CTC.
2. From the Tools menu, choose **Manage TL1 Tunnels**.

3. In the TL1 Tunnels window, view the information shown in Table 21-5.

Table 21-5: TL1 Tunnels Window

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

4. Return to your originating procedure (NTP).

DLP-D478 Edit a TL1 Tunnel Using CTC

Purpose	This task edits a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

1. From the Tools menu, choose **Manage TL1 Tunnels**.
2. In the TL1 Tunnels window, click the tunnel you want to edit.
3. Click **Edit**.
4. In the Edit CTC TL1 Tunnel dialog box, edit the following:
    - Use Default TL1 Port-Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
    - Use Other TL1 Port-Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
    - TL1 Encoding Mode-Choose the TL1 encoding:
        - LV + Binary Payload- TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
        - LV + Base64 Payload- TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
        - Raw-TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
    - GNE Login Required-Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
    - TID-If the GNE Login Required box is checked, enter the GNE TID.
5. Click **OK**.
6. If the GNE Login Required box is checked, complete login in the Login to Gateway NE dialog box. If not, continue Step 6.
    1. In the UID field, enter the TL1 user name.
    2. In the PID field, enter the TL1 user password.
    3. Click **OK**.
7. When the CTC Login dialog box appears, complete the CTC login. Refer to login procedures in the user documentation for the ONS ENE.
8. Return to your originating procedure (NTP).

DLP-D479 Delete a TL1 Tunnel Using CTC

Purpose	This task deletes a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

1. From the Tools menu, choose **Manage TL1 Tunnels**.
2. In the TL1 Tunnels window, click the tunnel you want to delete.

3. Click **Delete**.
4. In the confirmation dialog box, click **OK**.
5. Return to your originating procedure (NTP).

DLP-D480 Install or Reinstall the CTC JAR Files

Purpose	This task installs or reinstalls the CTC JAR files into the CTC cache directory on your PC. This is useful when you are using a new CTC version and want to install or reinstall the CTC JAR files without logging into a node or using the StartCTC application (StartCTC.exe).
Tools/Equipment	None
Prerequisite Procedures	NTP-D278 Set Up Computer for CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

1. Insert the Cisco ONS 15454 SDH Software Release 8.5 CD into your CD drive.
2. Navigate to the CacheInstall directory.
   Note: The CTC cache installer is also available on Cisco.com. If you are downloading the SetupCtc-*version*.exe (where *version* is the release version, for example, SetupCtc-085000.exe) file from Cisco.com, skip Step 1 and Step 2.
3. Copy the SetupCtc-*version*.exe file to your local hard drive. Use any location that is convenient for you to access, such as the Windows desktop. Ensure that you have enough disk space to copy and extract the SetupCtc-*version*.exe file.
4. Double-click the SetupCtc-*version*.exe file. This creates a directory named SetupCtc-*version* (at the same location), which contains the LDCACHE.exe file and other CTC files.
5. Double-click the LDCACHE.exe file to install or reinstall the new CTC JAR files into the CTC cache directory on your PC.
6. Return to your originating procedure (NTP).

DLP-D481 Configuring Windows Vista to Support CTC

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

1. Complete the following steps to disable Internet Explorer 7 protected mode:
   Note: Performa full installation of Windows Vista operating system on your computer. If Windows Vista is installed through operating system upgrade, then CTC will not work. Refer to the manufacturer's user guide for instructions on how to install Windows Vista.
   Note: If you start CTC by downloading the CTC Launcher application from the node then you do need to perform this procedure. See DLP-D473 Install the CTC Launcher Application from a Release 8.5 Node. This procedure is needed only if CTC is launched from the Internet Explorer browser.
   1. Open Internet Explorer,

2. Click **Tools > Internet Options**.
3. Click **Security** tab.
4. Select the zone that is appropriate. Available options are: **Local Intranet ,Internet, and Trusted Sites**.
5. Check the **Disable Protect Mode** check box.

2. Complete the following steps to Disable TCP Autotuning:
    1. From the Windows Start menu, click **Search > Search for Files and Folders**. The Search window appears.
    2. On the right side of the window in the Search box, type **Command Prompt** and press **Enter**. Windows will search for the Command Prompt application and list it in the search results.
    3. Right click **cmd** and select **Run as administrator**.
    4. Enter the administrator user ID and password and click **OK**.
    5. A Command prompt windows appears. At the command prompt enter the following text:
       `netsh interface tcp set global autotuninglevel=disabled`
       Autotuning can be enabled if desired using the following command:
       `netsh interface tcp set global autotuninglevel=normal`
3. Return to your originating procedure (NTP)

DLP-D482 Configure Link Integrity Timer

Purpose	This task sets the link integrity soak timer for each of the port in the Ethernet cards (mapper cards).
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In the node view, double-click a card to open the card view.
2. In the card view, click the **Provisioning > Ether Ports** tabs.
   Note: For the G1000 card, in the card view, click the **Provisioning > Port** tabs.
3. Change the Admin State of the port to Locked,Maintenance or Locked,Disabled for the corresponding port number.
4. In the Line area, enable the link integrity soak timer feature by unchecking the check box in the Link Integrity Disable column for the corresponding port number. The Link Integrity Disable option is available only for G1000 and CE-1000 cards.
5. Enter the desired link integrity soak duration in the Link Integrity Timer column for the corresponding port number. Enter the link integrity soak duration in the range between 200 and 5000 ms, in multiples of 100 ms.
   Note: The default link integrity timer value is 200 ms.
6. Click **Apply** to set the specified link integrity soak timer.
7. Return to your originating procedure (NTP).

DLP-D493 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

Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

1. In node view, double-click the ML-Series card where you want to provision the Ethernet port.
2. Click the **Provisioning > Ether Ports** tabs. The Ether Ports pane appears.
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.
    - 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.
4. Click **Apply**.
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:
    1. Click the **Performance > Ether Ports > Statistics** tabs.
    2. Click **Refresh**.
6. Return to your originating procedure (NTP).

DLP-D494 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
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

1. In node view, double-click the ML-Series card where you want to provision the POS port.
2. Click the **Provisioning > POS Ports** tabs. The POS Port pane appears.
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.

- 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.

4. Click **Apply**.
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:
    1. Click the **Performance > POS Ports > Statistics** tabs.
    2. Click **Refresh**.
6. Return to your originating procedure (NTP).