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

Contents

- 1 DLP-A507 View OC-N PM Parameters
  - 1.1 Figure 22-1: Viewing OC-N Card Performance Monitoring Information
- 2 DLP-A509 Provision CE-1000-4 Ethernet Ports
- 3 DLP-A510 Provision a DS-3 Circuit Source and Destination
- 4 DLP-A512 Change Node Access and PM Clearing Privilege
- 5 DLP-A513 Provision CE-100T-8 and CE-MR-10 Ethernet Ports
- 6 DLP-A514 Provision CE-100T-8, CE-1000-4, and CE-MR-10 POS Ports
- 7 DLP-A517 View Alarm or Event History
- 8 DLP-A518 Create a New or Cloned Alarm Severity Profile
  - 8.1 Figure 22-2: Node View Alarm Profile Editor
  - 8.2 Figure 22-3: Store Profiles Dialog Box
- 9 DLP-A519 Apply Alarm Profiles to Ports
  - 9.1 Figure 22-4: DS1-N-14 Card Alarm Behavior Tab
- 10 DLP-A520 Delete Alarm Severity Profiles
  - 10.1 Figure 22-5: Select Node/Profile Combination For Delete Dialog Box
- 11 DLP-A521 Modify Alarm, Condition, and History Filtering Parameters
  - 11.1 Figure 22-6: Alarm Filter Dialog Box General Tab
  - 11.2 Figure 22-7: Alarm Filter Dialog Box Conditions Tab
- 12 DLP-A522 Suppress Alarm Reporting
- 13 DLP-A523 Discontinue Alarm Suppression
- 14 DLP-A524 Download an Alarm Severity Profile
- 15 DLP-A526 Change Line and Threshold Settings for the DS3i-N-12 Cards
  - 15.1 Table 22-1: Line Options for the DS3i-N-12 Cards
  - 15.2 Table 22-2: Line Threshold Options for the DS3i-N-12 Cards
  - 15.3 Table 22-3: Electrical Path Options for the DS3i-N-12 Cards
  - 15.4 Table 22-4: SONET Threshold Options for DS3i-N-12 Cards
- 16 DLP-A527 Change the OC-N Card ALS Maintenance Settings
  - 16.1 Table 22-5: OC-N Maintenance Settings
- 17 DLP-A528 Change the Default Network View Background Map
- 18 DLP-A529 Delete Ethernet RMON Alarm Thresholds
- 19 DLP-A530 Install the Tie-Down Bar
  - 19.1 Figure 22-8: Tie-Down Bar
- 20 DLP-A531 Print CTC Data
  - 20.1 Figure 22-9: Selecting CTC Data For Print
- 21 DLP-A532 Export CTC Data
  - 21.1 Figure 22-10: Selecting CTC Data For Export
- 22 DLP-A533 Create Ethernet RMON Alarm Thresholds
  - 22.1 Figure 22-11: Creating RMON Thresholds
  - 22.2 Table 22-6: Ethernet Threshold Variables (MIBs)
  - 22.3 Table 22-7: POS Threshold Variables (MIBs)
- 23 DLP-A534 Provision OSI Routing Mode
- 24 DLP-A535 Provision or Modify TARP Operating Parameters
- 25 DLP-A536 Add a Static TID to NSAP Entry to the TARP Data Cache
- 26 DLP-A537 Remove a Static TID to NSAP Entry from the TARP Data Cache

- 27 DLP-A538 Add a TARP Manual Adjacency Table Entry
- 28 DLP-A539 Provision OSI Routers
- 29 DLP-A540 Provision Additional Manual Area Addresses
- 30 DLP-A541 Enable the OSI Subnet on the LAN Interface
- 31 DLP-A542 Create an IP-Over-CLNS Tunnel
- 32 DLP-A543 Remove a TARP Manual Adjacency Table Entry
- 33 DLP-A544 Change the OSI Routing Mode
- 34 DLP-A545 Edit the OSI Router Configuration
- 35 DLP-A546 Edit the OSI Subnetwork Point of Attachment
- 36 DLP-A547 Edit an IP-Over-CLNS Tunnel
- 37 DLP-A548 Delete an IP-Over-CLNS Tunnel
- 38 DLP-A549 View IS-IS Routing Information Base
- 39 DLP-A550 View ES-IS Routing Information Base
- 40 DLP-A551 Manage the TARP Data Cache
- 41 DLP-A552 Adjust the Java Virtual Memory Heap Size
- 42 DLP-A553 Upgrade DS1 or DS3-12 Cards in a 1:N or 1:1 Configuration to High-Density Electrical Cards
- 43 DLP-A553 Upgrade DS3XM-6 Cards in a 1:1 Configuration to High-Density DS3XM-12 Electrical Cards
- 44 DLP-A554 Upgrade EC-1 Cards in a 1:1 Configuration to DS3/EC1-48 Cards
- 45 DLP-A555 Set Up SDH External or Line Timing
- 46 DLP-A556 Provision the Card Mode for ML-Series Ethernet Cards
- 47 DLP-A557 View Multirate PM Parameters
- 48 DLP-A558 Provision the Designated SOCKS Servers
- 49 DLP-A559 Install or Reinstall the CTC JAR Files
- 50 DLP-A560 Create an Optimized 1+1 Protection Group
- 51 DLP-A561 Modify an Optimized 1+1 Protection Group
- 52 DLP-A562 View ML-Series RPR Span PM Parameters
- 53 DLP-A563 Configure an Automatically Routed BLSR DRI
    - 53.1 Figure 22-12: Selecting BLSR DRI Primary and Secondary Node Assignments
- 54 DLP-A564 Configure a Manually Routed BLSR DRI
    - 54.1 Figure 22-13: Selecting BLSR DRI Primary and Secondary Node Assignments (Manual Routing)
- 55 DLP-A565 Set Up a Solaris Workstation for a Craft Connection to an ONS 15454
- 56 DLP-A566 Install the CTC Launcher Application from a Release 8.5 Software CD
- 57 DLP-A567 Install the CTC Launcher Application from a Release 8.5 Node
- 58 DLP-A568 Connect to ONS Nodes Using the CTC Launcher
    - 58.1 Figure 22-14: CTC Launcher Window
- 59 DLP-A569 Create a TL1 Tunnel Using the CTC Launcher
- 60 DLP-A570 Create a TL1 Tunnel Using CTC
- 61 DLP-A571 View TL1 Tunnel Information
    - 61.1 Table 22-8: TL1 Tunnels Window
- 62 DLP-A572 Edit a TL1 Tunnel Using CTC
- 63 DLP-A573 Delete a TL1 Tunnel Using CTC
- 64 DLP-A574 Provision a PPM on the MRC-12 or MRC-2.5G-4 Card
- 65 DLP-A575 Provision the Optical Line Rate on the MRC-12 or MRC-2.5G-4 Card
    - 65.1 Table 22-9: PPM Port Types
- 66 DLP-A576 Change the Optical Line Rate on the MRC-12 or MRC-2.5G-4 Card
- 67 DLP-A577 Delete a PPM from the MRC-12, MRC-2.5G-4, or OC192-XFP Card
- 68 DLP-A578 Configuring Windows Vista to Support CTC
- 69 DLP-A579 Provision an Open VCAT Circuit Source and Destination
- 70 DLP-A580 Create User Defined Alarm Types
- 71 DLP-A 581 Configure Link Integrity Timer

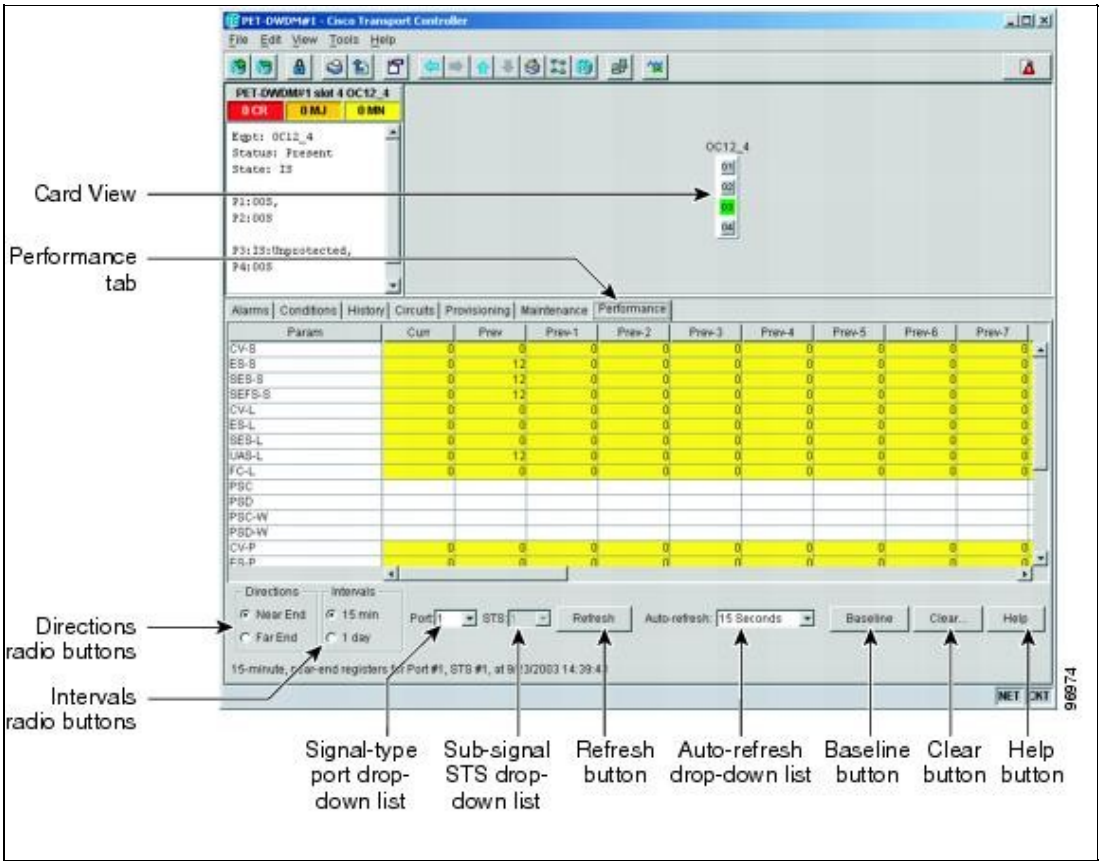
• 72 DLP-A595 Provision Card Mode for CE-MR-10 Card

DLP-A507 View OC-N PM Parameters

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

1. In node view, double-click the OC-N card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab (Figure 22-1).

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



3. In the Port drop-down list, click the port 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 Reference Manual*.
6. To monitor another port on a multiport card, choose another port from the Port drop-down list and click **Refresh**.
7. Return to your originating procedure (NTP).

DLP-A509 Provision CE-1000-4 Ethernet Ports

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

Note: You can provision SONET contiguous concatenated (CCAT) or virtual concatenated (VCAT) circuits for the CE-1000-4 before or after provisioning the card's Ethernet ports and/or packet-over-SONET (POS) ports. See the NTP-A343 Create an Automatically Routed Optical Circuit or the NTP-A264 Create an Automatically Routed VCAT Circuit, as needed.

1. In node view, double-click the CE-1000-4 card graphic to open the card.
2. Click the **Provisioning > Ether Ports** tabs.
3. For each CE-1000-4 port, provision the following parameters:
   - Port Name- If you want to label the port, enter the port name.
   - Admin State- Select the service state for the port. See the "DLP-A214 Change the Service State for a Port" task for more information.
     Note: CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.
   - Flow Control- Select the flow control for the port. Possible values are **None**, **Symmetrical**, and **Pass Through**.
   - Auto Negotiation- Click this check box to enable autonegotiation on the port (default). If you do not want to enable autonegotiation control, uncheck the box.
   - MTU- If you want to permit the acceptance of jumbo size Ethernet frames, choose 10004(default). If you do not want to permit jumbo size Ethernet frames, choose 1548.
   - Watermark- Select the flow control watermark for the port. To provision the Low Latency flow control watermark, choose **Low Latency** from the drop-down list. The Flow Ctrl Lo and Flow Ctrl Hi values change. To provision a Custom flow control watermark, choose **Custom** from the drop-down list. Enter values in the Flow Ctrl Hi and Flow Ctrl Lo columns. The Flow Ctrl Lo value has a valid range from 1 to 510 and the Flow Ctrl Hi value has a valid range from 2 to 511. The Flow Ctrl Lo value must be lower than the Flow Ctrl Hi value.
4. Click **Apply**.
5. Refresh the Ethernet statistics:
   1. Click the **Performance > Ether Ports > Statistics** tabs.
   2. Click **Refresh**.
      Note: Reprovisioning an Ethernet port on the CE-1000-4 card does not reset the Ethernet statistics for that port.
6. Return to your originating procedure (NTP).

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

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

Security Level	Provisioning or higher

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

1. From the Node drop-down list, choose the node where the source will originate.
2. From the Slot drop-down list, choose the slot containing the DS-3 card where the circuit will originate. If you are configuring a DS-3 circuit with a transmux card, choose the DS3XM-6 or DS3XM-12 card.
3. From the Port drop-down list, choose the source DS-3, DS3/EC1-48, DS3XM-6, or DS3XM-12 card as appropriate.
4. If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection configuration, click **Use Secondary Source** and repeat Steps 1 through 3 to define the secondary source. If you do not need to create a secondary source, continue with Step 5.
5. Click **Next**.
6. From the Node drop-down list, choose the destination (termination) node.
7. From the Slot drop-down list, choose the slot containing the destination card. The destination is typically a DS3XM-6 or DS-3 card. You can also choose an OC-N card to map the DS-3 circuit to a synchronous transport signal (STS).
8. Depending on the destination card, choose the destination port or STS from the drop-down lists that appear based on the card selected in Step 2. See Table 6-2 for a list of valid options. Cisco Transport Controller (CTC) does not display ports, STSs, Virtual Tributaries (VTs), or DS3s if they are already in use by other circuits. If you and another user who is working on the same network choose the same port, STS, VT, port, or DS3 simultaneously, one of you receives a Path in Use error and is unable to complete the circuit. The user with the partial circuit needs to choose new destination parameters.
9. If you need to create a secondary destination, for example, a path protection bridge/selector circuit exit point in a multivendor path protection configuration, click **Use Secondary Destination** and repeat Steps 6 through 8 to define the secondary destination.
10. Click **Next**.
11. Return to your originating procedure (NTP).

DLP-A512 Change Node Access and PM Clearing Privilege

Purpose	This task provisions the physical access points and shell programs used to connect to the ONS 15454 and sets the user security level that can clear node PM data.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
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), 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 EMS access state from the list. Available states are Non-Secure and Secure (allows access using SSH).

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

   - ♦ **Default - TCC Fixed**-Uses Port 57790 to connect to ONS 15454s on the same side of the firewall or if no firewall is used (default). This option can be used for access through a firewall if Port 57790 is open.
   - ♦ **Standard Constant**-Uses Port 683 (IIOP) or Port 684 (SSLIOP), the Common Object Request Broker Architecture (CORBA) default port number.
   - ♦ **Other Constant**-If the default port is not used, type the Internet Inter-ORB Protocol (IIOP) or SSLIOP port specified by your firewall administrator.
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-A513 Provision CE-100T-8 and CE-MR-10 Ethernet Ports

Purpose	This task provisions CE-100T-8 and CE-MR-10 Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: You can provision SONET contiguous concatenated (CCAT) or virtual concatenated (VCAT) circuits for the CE-100T-8 and CE-MR-10 cards before or after provisioning the card's Ethernet ports and/or packet-over-SONET (POS) ports. See the NTP-A343 Create an Automatically Routed Optical Circuit or the NTP-A264 Create an Automatically Routed VCAT Circuit, as needed.

1. In node view, double-click the CE-100T-8 or CE-MR-10 card graphic to open the card.
2. Click the **Provisioning > Ether Ports** tabs.
3. For each CE-100T-8 or CE-MR-10 port, provision the following parameters:
   - Port Name-If you want to label the port, enter the port name.
   - Admin State-Choose **IS** to put the port in service.
   - Expected Speed-Choose the expected speed of the device that is or will be attached to the Ethernet port. If you know the speed, choose 100 Mbps or 10 Mbps (for CE-100T-8), or 1000 Mbps, 100 Mbps, or 10 Mbps (for CE-MR-10) to match the attached device. If you do not know the speed, choosing Auto enables autonegotiation for the speed of the port, and the CE-100T-8 or CE-MR-10 port will attempt to negotiate a mutually acceptable speed with the attached device. If the expected speed is set to Auto, you cannot enable selective autonegotiation.
   - Expected Duplex-Choose the expected duplex of the device that is or will be attached to the Ethernet port. If you know the duplex, choose Full or Half to match the attached device. If you do not know the duplex, choosing Auto enables autonegotiation for the duplex of the port, and the CE-100T-8 or CE-MR-10 port will attempt to negotiate a mutually acceptable duplex with the attached device. If the expected duplex is set to Auto, you cannot enable selective autonegotiation.
   - Enable Selective Auto Negotiation-Click this check box to enable selective autonegotiation on the Ethernet port. If you do not want to enable selective autonegotiation, uncheck the box. If checked, the CE-100T-8 or CE-MR-10 port attempts to autonegotiate only to the selected expected speed and duplex. The link will come up if both the expected speed and duplex of the attached autonegotiating device matches that of the port. You cannot enable selective autonegotiation if either the expected speed or expected duplex is set to Auto.
   - Enable Flow Control-Click this check box to enable flow control on the port (default). If you do not want to enable flow control, uncheck the box. The CE-100T-8 or CE-MR-10 card attempts to negotiate symmetrical flow control with the attached device.
   - 802.1Q VLAN CoS-For a class-of-service (CoS)-tagged frame, the CE-100T-8 or CE-MR-10 card can map the eight priorities specified in CoS for either priority or best effort treatment. Any CoS class higher than the class specified in CTC is mapped to priority, which is the treatment geared towards low latency. By default, the CoS is set to 7, which is the highest CoS value. The default results in all traffic being treated as best effort.
   - IP ToS-The CE-100T-8 or CE-MR-10 card can also map any of the 256 priorities specified in IP type-of-service (ToS) to either priority or best effort treatment. Any ToS class higher than the class specified in CTC is mapped to priority, which is the treatment geared towards low latency. By default, the ToS is set to 255, which is the highest ToS value. This results in all traffic being sent to the best effort queue by default.
     Note: Untagged traffic is treated as best effort.
     Note: If traffic is tagged with both CoS and IP ToS, then the CoS value is used, unless the CoS value is 7.
4. Click **Apply**.
5. Refresh the Ethernet statistics:
   1. Click the **Performance > Ether Ports > Statistics** tabs.
   2. Click **Refresh**.
      Note: Reprovisioning an Ethernet port on the CE-100T-8 or CE-MR-10 card does not reset the Ethernet statistics for that port.

6. Return to your originating procedure (NTP).

DLP-A514 Provision CE-100T-8, CE-1000-4, and CE-MR-10 POS Ports

Purpose	This task provisions CE-100T-8, CE-1000-4, or CE-MR-10 POS ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: You can provision SONET CCAT or VCAT circuits for the CE-Series card before or after provisioning the card's Ethernet ports and/or POS ports. See the NTP-A343 Create an Automatically Routed Optical Circuit or the NTP-A264 Create an Automatically Routed VCAT Circuit, as needed.

1. In node view, double-click the CE-100T-8, CE-1000-4, or CE-MR-10 card graphic to open the card.
2. Click the **Provisioning > POS Ports** tabs.
3. For each CE-100T-8, CE-1000-4, or CE-MR-10 port, provision the following parameters:
   - Port Name-If you want to label the port, enter the port name.
   - Admin State-Choose **IS** to put the port in service.
   - Framing Type-Choose GPF-F POS framing (the default) or HDLC POS framing. The framing type needs to match the framing type of the POS device at the end of the SONET circuit.
   - Encap CRC-With GFP-F framing, the user can configure a 32-bit cyclic redundancy check (CRC) (the default) or none (no CRC). HDLC framing provides a set 32-bit CRC. The CRC should be set to match the CRC of the POS device on the end of the SONET circuit.
     Note: For more details about the interoperabilty of Optical Networking System (ONS) Ethernet cards, including information on encapsulation, framing, and CRC, refer to the "POS on ONS Ethernet Cards" chapter of the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.
     Note: The CE-Series cards use LEX encapsulation, which is the primary POS encapsulation used in ONS Ethernet cards.
4. Click **Apply**.
5. Refresh the POS statistics:
   1. Click the **Performance > POS Ports > Statistics** tabs.
   2. Click **Refresh**.
6. Return to your originating procedure (NTP).

DLP-A517 View Alarm or Event History

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

Security Level	Retrieve or higher

1. Decide whether you want to view the alarm message history at the 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.
        If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.
    3. Click **Retrieve** to view all available messages for the **History > Shelf** tabs.
        Note: Alarms can be unreported when they are filtered out of the display using the Filter button in either tab. See the "DLP-A225 Enable Alarm Filtering" task for information.

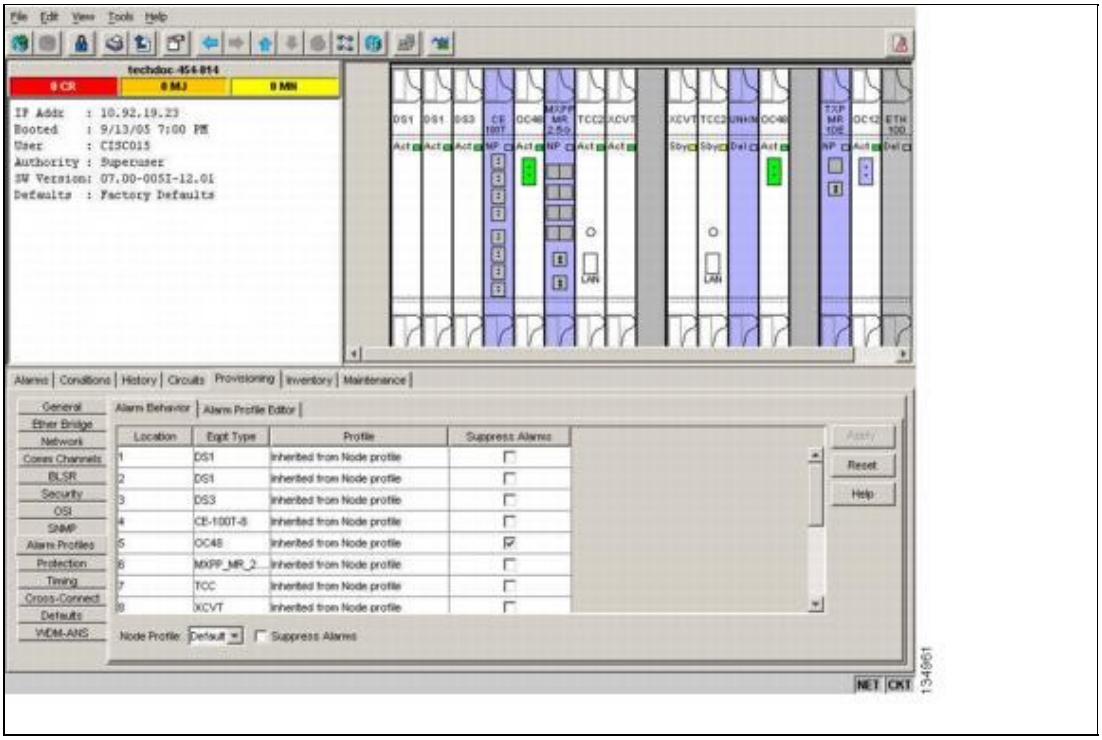
    Tip: Double-click an alarm in the alarm table or an event (condition) message in the history table to display the view that corresponds to the alarm message. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.
3. To view 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**.
    2. Double-click a card on the shelf graphic to open the card-level view.
        Note: TCC2/TCCP cards and cross-connect (XCVT, XC10G, or XC-VXL-10G) cards do not have a card view.
    3. Click the **History > Session** tab to view the alarm messages raised during the current session.
    4. Click the **History > Card** tab to retrieve all available alarm messages for the card and click **Retrieve**.
        If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.
        Note: The ONS 15454 can store up to 640 critical alarm messages, 640 major alarm messages, 640 minor alarm messages, and 640 condition messages. When any of these limits is reached, the ONS 15454 discards the oldest events in that category.
        Raised and cleared alarm messages (and events, if selected) appear.
5. Return to your originating procedure (NTP).

DLP-A518 Create a New or Cloned Alarm Severity Profile

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

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

Figure 22-2: Node View Alarm Profile Editor



3. To access the profile editor from a card view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
4. If you want to create a new profile based upon the default profile in use, click **New**. Then go to Step 10.
5. If you want to create a profile using an existing profile located on the node, click **Load** and **From Node** in the Load Profile(s) dialog box.
    1. Click the node name you are logged into in the Node Names list.
    2. Click the name of an existing profile in the Profile Names list, such as **Default**. Then go to Step 7.
6. If you want to create a profile using an existing profile located in a file that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.
    1. Click **Browse**.
    2. Navigate to the file location in the **Open** dialog box.
    3. 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.
7. Click **OK**.

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

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

(Refer to Step 11 for further information about the Default profile.)

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

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

10. In the New Profile or Clone Profile dialog box, enter a name in the New Profile Name field. Profile names must be unique. If you try to import or name a profile that has the same name as another profile, CTC adds a suffix to create a new name. Long file names are supported.
11. Click **OK**.

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

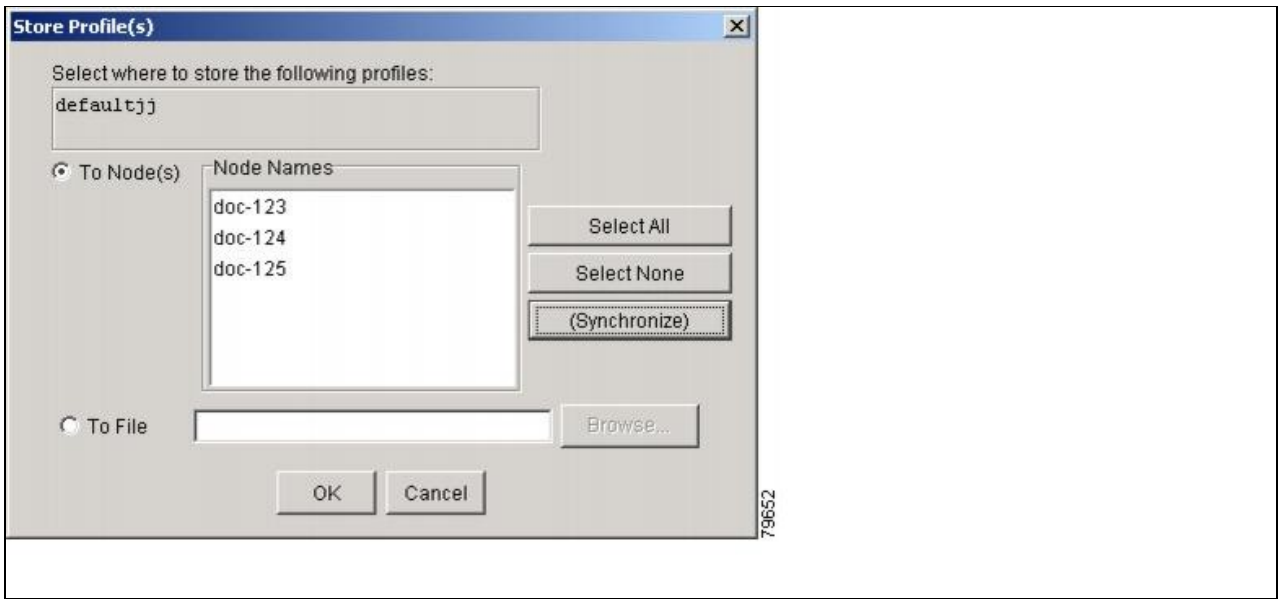
    Note: Up to 10 profiles, including the two reserved profiles, Inherited and Default, can be stored in CTC.

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

12. Modify (customize) the new alarm profile:
    1. In the new alarm profile column, 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 for each severity you want to customize. Refer to the following guidelines when you view the alarms or conditions after making modifications:

       - All Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.
       - Default severities are used for all alarms and conditions until you create and apply a new profile.
       - Changing a severity to inherited (I) or unset (U) does not change the severity of the alarm.
13. After you have customized the new alarm profile, right-click the profile column to highlight it.
14. Click **Store**.
15. In the Store Profile(s) dialog box, click **To Node(s)** and go to Substep 1 or click **To File** and go to Substep 2 (Figure 22-3).

    Figure 22-3: Store Profiles Dialog Box



1. Choose the nodes where you want to save the profile:
   - If you want to save the profile to only one node, click the node in the Node Names list.
   - If you want to save the profile to all nodes, click **Select All**.
   - If you do not want to save the profile to any nodes, click **Select None**.
   - If you want to update alarm profile information, click **(Synchronize)**.
2. Save the profile:
   - Click **Browse** and navigate to the profile save location.
   - Enter a name in the File name field.
   - Click **Select** to choose this name and location. Long file names are supported. CTC supplies a suffix of *.pfl to stored files.
   - Click **OK** to store the profile.

16. As needed, perform any of the following actions:
    - ♦ Click the **Hide Identical Rows** check box to configure the Alarm Profiles window to view rows with dissimilar severities.
    - ♦ Click the **Hide Reference Values** check box to configure the Alarm Profiles window to view severities that do not match the Default profile.
    - ♦ Click the **Only show service-affecting severities** check box to configure the Alarm Profiles window not to display Minor and some Major alarms that will not affect service.
17. Return to your originating procedure (NTP).

DLP-A519 Apply Alarm Profiles to Ports

Purpose	This task applies a custom or default alarm severity profile to a port or ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A518 Create a New or Cloned Alarm Severity Profile DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Figure 22-3: Store Profiles Dialog Box

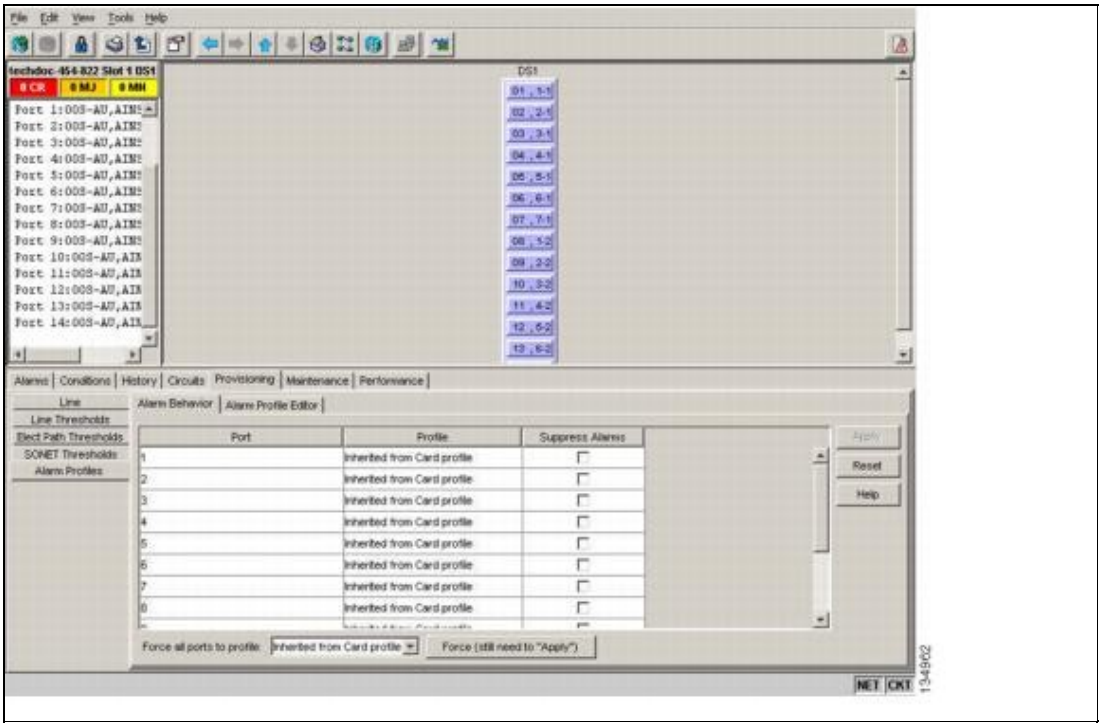
1. In the node view, double-click a card to open the card view.

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

   Note: The card view is not available for the TCC2/TCCP or cross-connect cards.
2. Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

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

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



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

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 18-3).
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-A520 Delete Alarm Severity Profiles

Purpose	This task deletes a custom or default alarm severity profile.

Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. To access the alarm profile editor from network view, go to network view and click the **Provisioning > Alarm Profiles** tabs.
2. To access the profile editor from node view, go to node view and click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
3. To access the profile editor from a card view, double-click the card to display the card view and click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
4. Click the profile you are deleting to select it.
5. Click **Delete**.

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

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

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

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

   Tip: If you hold the Shift key down, you can select consecutive node names. If you hold the Ctrl key down, you can select any combination of nodes.
7. Click the profile names you want to delete in the Profile Names list.
8. Click **OK**.

   Click **Yes** in the Delete Alarm Profile dialog box.
   Note: If you delete a profile from a node, it still appears in the network view Provisioning > Alarm Profile Editor window unless you remove it using the following step.
9. To remove the alarm profile from the window, right-click the column of the profile you deleted and choose **Remove** from the shortcut menu.

   Note: If a node and profile combination is selected but does not exist, a warning appears: "One or more of the profile(s) selected do not exist on one or more of the node(s) selected."

For example, if node A has only profile 1 stored and the user tries to delete both profile 1 and profile 2 from node A, this warning appears. However, the operation still removes profile 1 from node A.

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

10. Return to your originating procedure (NTP).

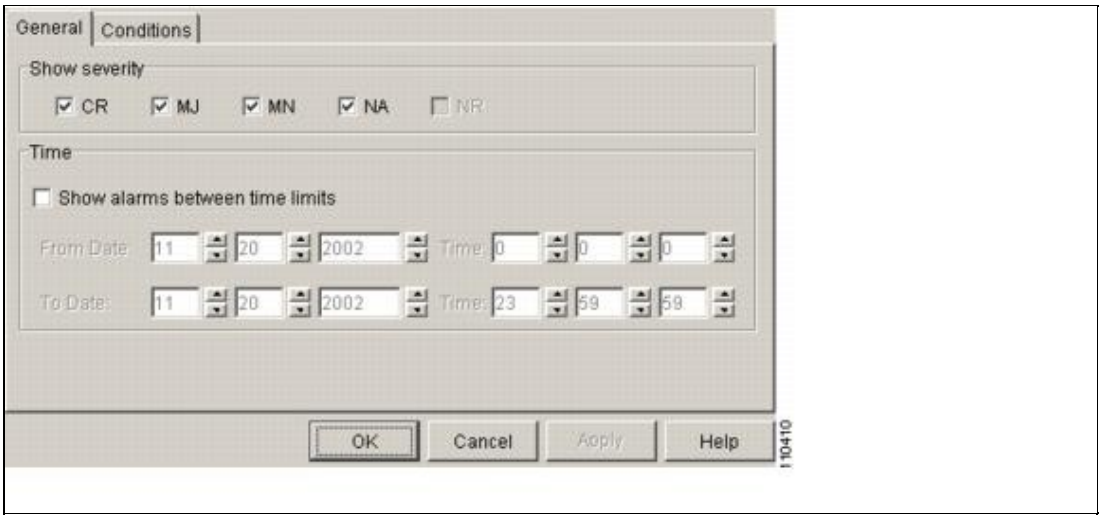
DLP-A521 Modify Alarm, Condition, and History Filtering Parameters

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

1. At the node, network, or card view, click the **Alarms** tab, Conditions tab, 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 22-6 shows the Alarm Filter dialog box; the Conditions and History tabs have similar dialog boxes.

Figure 22-6: Alarm Filter Dialog Box General Tab



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

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

   When alarm filtering is disabled, all alarms show.
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 22-7).

Figure 22-7: Alarm Filter Dialog Box Conditions Tab

Output/110409.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-A225 Enable Alarm Filtering" task), and the parameters are not enforced when alarm filtering is disabled (see the "DLP-A227 Disable Alarm Filtering" task).

7. Return to your originating procedure (NTP).

DLP-A522 Suppress Alarm Reporting

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

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

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

1. If you are in 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, and the word System will appear in the Object column.

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

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.
       Alarms that directly apply to this card will change appearance as described in Step 2. For example, if you suppressed raised alarms for an OC-48 card in Slot 16, raised alarms for this card will change in node or card view. The AS-CMD alarm will show the slot number in the Object number. For example, if you suppressed alarms for a Slot 16 OC-48 card, the AS-CMD object will be "SLOT-16."
       Click **Apply**.
4. To suppress alarms for individual card ports, double-click the card in node view.
5. Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
6. Check the **Suppress Alarms** column check box for the port row where you want to suppress alarms (Figure 22-4).
7. Click **Apply**.
   Alarms that apply directly to this port will change appearance as described in Step 2. (However, alarms raised on the entire card will remain raised.) A raised AS-CMD alarm that shows the port as its object will appear in either alarm window. For example, if you suppressed alarms for Port 1 on the Slot 16 OC-48 card, the alarm object will show "FAC-16-1."
8. Return to your originating procedure (NTP).

DLP-A523 Discontinue Alarm Suppression

Purpose	This task discontinues alarm suppression and reenables alarm reporting on a port, card, or node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A522 Suppress Alarm Reporting DLP-A60 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** tab.
    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, double-click the card to open the card view and click the

Provisioning > Alarm Profiles > Alarm Behavior tabs.

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-A524 Download an Alarm Severity Profile

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

1. To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.
2. To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
3. To access the profile editor from a card view, double-click the card to open the card view and click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
4. Click **Load**.
5. If you want to download a profile that exists on the node, click **From Node** in the Load Profile(s) dialog box.
   1. Click the node name you are logged into in the Node Names list.
   2. Click the name of the profile in the Profile Names list, such as **Default**.
6. If you want to download a profile that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.
   1. Click **Browse**.
   2. Navigate to the file location in the **Open** dialog box.
   3. Click **Open**.

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

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

   The downloaded profile appears at the right side of the Alarm Profiles window.
8. Right-click anywhere in the downloaded profile column to view the profile editing shortcut menu.
9. Click **Store**.
10. In the Store Profile(s) dialog box, click **To Node(s)**.

    1. Choose the nodes where you want to save the profile:

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

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

11. **Click OK**.

11. Return to your originating procedure (NTP).

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

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

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

1. In node view, double-click the DS3i-N-12 card where you want to change the line or threshold settings.
2. Click the **Provisioning** tab.
3. Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, or **SONET Thresholds** subtab.
   Note: See Manage Alarms for information about the Alarm Profiles tab.
   Note: If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.
4. Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.
5. Click **Apply**.
6. Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.
   For definitions of the line settings, see Table 22-1. For definitions of the line threshold settings, see Table 22-2. For definitions of the electrical path threshold settings, see Table 22-3. For definitions of the SONET threshold settings, see Table 22-4.

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

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

Parameter	Description	Options
Port	(Display only) Port number.	1 to 12
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6

		• 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• Unframed • M13 • C Bit • Auto Provisioned
Detected Line Type	Displays the detected line type.	• M13 • C Bit • Unframed • Unknown
Line Coding	(Display only) Defines the DS3E transmission coding type.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
Admin State	Sets the port administrative service state unless network conditions prevent the change.	• IS-Puts the port in-service. The port service state changes to IS-NR. • IS,AINS-Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD-Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT-Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note:** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR-(In-Service and Normal) The port is fully operational and performing as provisioned. • OOS-AU,AINS-(Out-Of-Service and Autonomous, Automatic In-Service) The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD-(Out-of-Service and Management, Disabled) The port is out-of-service and unable to carry traffic. • OOS-MA,MT-(Out-of-Service and Management, Maintenance) The port is out-of-service for maintenance.

		Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

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

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

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

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

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

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

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

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

Parameter	Description
Port	(Display only) Port number; 1 to 12
CV	Coding violations
ES	Errored seconds
FC	Failure count
SES	Severely errored seconds
UAS	Unavailable seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Note: The threshold value appears after the circuit is created.

7. Return to your originating procedure (NTP).

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

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

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

1. In node view, double-click the OC-N card where you want to change the ALS maintenance settings.
2. Click the **Maintenance > ALS** tabs.
3. Modify any of the settings described in Table 22-5 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box. The provisionable parameters are listed in the options column in the table.
4. Click **Apply**. If the change affects traffic, a warning message displays. Click Yes to complete the change.

Table 22-5: OC-N Maintenance Settings

Parameter	Description	Options
Port number	(Display only) Port number	-
ALS Mode	Automatic laser shutdown mode. ALS provides the ability to shut down the TX laser when the RX detects a loss of	From the drop-down list, choose one of the following:

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

5. Return to your originating procedure (NTP).

DLP-A528 Change the Default Network View Background Map

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

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. In the node view, click the **Provisioning > Defaults** tabs.
3. In the Defaults Selector area, choose **CTC** and then **network**.
4. Click the **Default Value** field and choose a default map from the drop-down list. Map choices are: Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).

5. Click **Apply**. The new network map appears.
6. Click **OK**.
7. If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the ONS 15454 icons are visible. (You can also choose **Fit Graph to Window**.)
8. If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.
9. If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.
10. Return to your originating procedure (NTP).

DLP-A529 Delete Ethernet RMON Alarm Thresholds

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

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

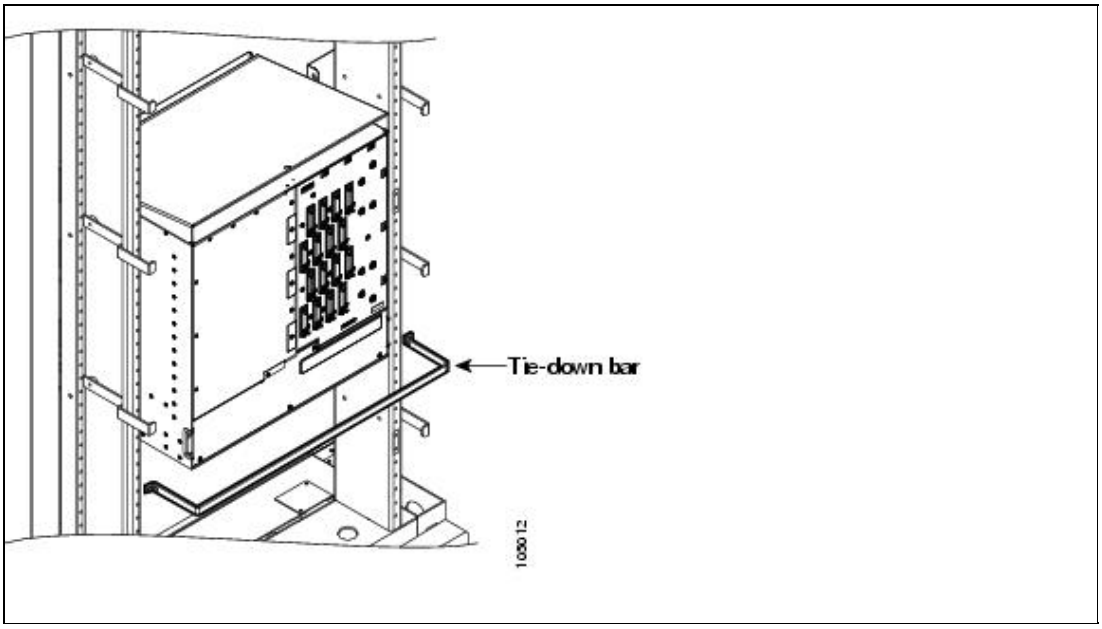
1. Double-click the Ethernet card where you want to delete the RMON alarm thresholds.
2. In card view, click the **Provisioning > Ether Ports > RMON Thresholds** tabs.
   Note: For the CE-Series, click the **Provisioning > Ether Ports > RMON Thresholds** tabs or **Provisioning > POS Ports > RMON Thresholds**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

DLP-A530 Install the Tie-Down Bar

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

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

Figure 22-8: Tie-Down Bar



2. Install the four screws into the rack.
3. Return to your originating procedure (NTP).

DLP-A531 Print CTC Data

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

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

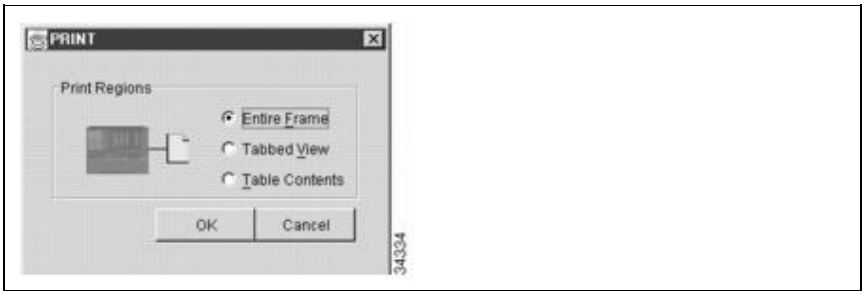
   The print operation is available for all network, node, and card view windows.
2. From the File menu choose **Print**.
3. In the Print dialog box, click a printing option (Figure 22-9).
   - Entire Frame-Prints the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.
   - Tabbed View-Prints the lower half of the CTC window containing tabs and data. The printout includes the selected tab (on top) and the data shown in the tab window. For example, if you print the History window Tabbed View, you print only history items appearing in the window. This option is available for all windows.
   - Table Contents-Prints CTC data in table format without graphical representations of shelves, cards, or tabs. This option does not apply to the following windows:
     - Provisioning > General tab (General, Power Monitor, and Multishelf Config) windows
     - Provisioning > Network > General window
     - Provisioning > Security > Policy, Access, and Legal Disclaimer windows

◊ Provisioning > SNMP window
◊ Provisioning > Timing > General and BITS Facilities windows
◊ Provisioning > Cross-Connect window
◊ Provisioning > OSI > Main Setup window and OSI > TARP > Config window
◊ Provisioning > Comm Channels > LMP > General window
◊ Provisioning > WDM-ANS > Node Setup window
◊ Maintenance > Cross-Connect > Cards window
◊ Maintenance > Database window
◊ Maintenance > Diagnostic window
◊ Maintenance > Protection window
◊ Maintenance > Timing > Source window
◊ Maintenance > DWDM > ROADM Power Monitoring window

The Table Contents option prints all the data contained in a table and the table column headings. For example, if you print the History window Table Contents view, you print all data included in the table whether or not items appear in the window.

Tip: When you print using the Tabbed View option, it can be difficult to distinguish whether the printout applies to the network, node, or card view. To determine the view, compare the tabs on the printout. The network, node, and card views are identical except that network view does not contain an Inventory tab or Performance tab.

Figure 22-9: Selecting CTC Data For Print



4. Click **OK**.
5. In the Windows Print dialog box, click a printer and click **OK**.
6. Repeat this task for each window that you want to print.
7. Return to your originating procedure (NTP).

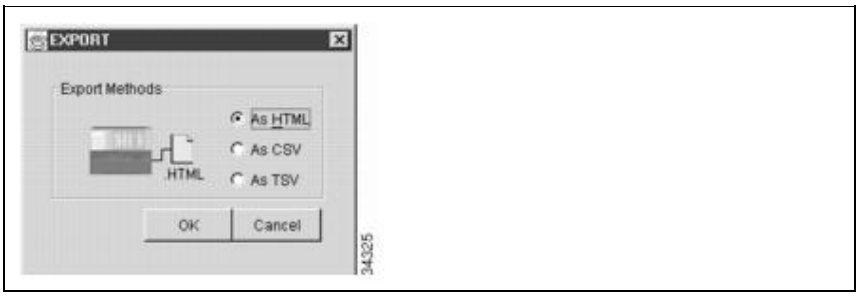
DLP-A532 Export CTC Data

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

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

2. If you want to export detailed circuit information, complete the following:
    1. In the Circuits window, choose a circuit and click **Edit** to open it in the Edit Circuits window.
    2. In the Edit Circuits window, choose the desired tab: Drops, Path Protection Selectors, Path Protection Switch Counts, State, or Merge. (Depending on your configuration, you may or may not see all of these tabs.)
3. From the File menu, choose **Export**.
4. In the Export dialog box, click a data format (Figure 22-10):
    - **As HTML**-Saves data as a simple HTML table file without graphics. The file must be viewed or edited with applications such as Netscape Navigator, Microsoft Internet Explorer, or other applications capable of opening HTML files.
    - **As CSV**-Saves the CTC table as comma-separated values (CSV). This option does not apply to the Maintenance > Timing > Report window.
    - **As TSV**-Saves the CTC table as tab-separated values (TSV).

Figure 22-10: Selecting CTC Data For Export



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

    Text editor and word processor applications format the data exactly as it is exported, including comma or tab separators. All applications that open the data files allow you to format the data.
6. If you want to open the file in spreadsheet and database management applications, procedures vary. Typically, you need to open the application and choose File > Import, then choose a delimited file to format the data in cells.

    Spreadsheet and database management programs also allow you to manage the exported data.
    Note: An exported file cannot be opened in CTC.
    The export operation does not apply to the following windows:
    - Provisioning > General > General, Power Monitor, and Multishelf Config window
    - Provisioning > Network > General window
    - Provisioning > Security > Policy, Access, and Legal Disclaimer window
    - Provisioning > SNMP window
    - Provisioning > Timing > General and BITS FAcilities windows
    - Provisioning > OSI > Main Setup window and OSI > TARP > Config window
    - Provisioning > Comm Channels > LMP > General window
    - Provisioning > Cross-Connect window
    - Provisioning > WDM-ANS > Node Setup window
    - Maintenance > Cross-Connect > Cards window
    - Maintenance > Database window
    - Maintenance > Diagnostic window

· Maintenance > Protection window
· Maintenance > Timing > Source window
· Maintenance > DWDM > ROADM Power Monitoring window

7. Click **OK**.
8. In the Save dialog box, enter a name in the File name field using one of the following formats:

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

9. Navigate to a directory where you want to store the file.
10. Click **OK**.
11. Repeat the task for each window that you want to export.
12. Return to your originating procedure (NTP).

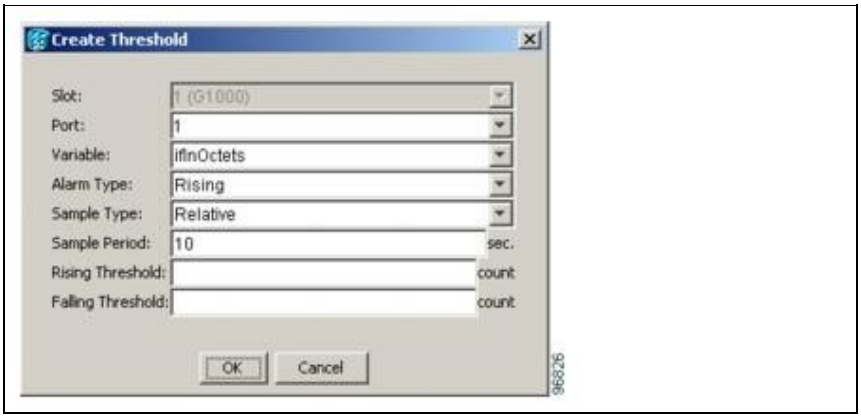
DLP-A533 Create Ethernet RMON Alarm Thresholds

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

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

1. Complete the "DLP-A60 Log into CTC" task at the node where you want to set up RMON. If you are already logged in, continue with Step 2.
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.
   Note: For CE- and ML-Series Ethernet cards, click the **Provisioning > Ether Ports > RMON Thresholds** tabs or **Provisioning > POS Ports > RMON Thresholds** tabs.
4. Click **Create**.
   The Create Ether Threshold dialog box appears (Figure 22-11).

Figure 22-11: Creating RMON Thresholds



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

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

Table 22-6: Ethernet Threshold Variables (MIBs)

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

	(Not supported by E-Series or G-Series) Number of times that a collision was detected later than 64 octets into the transmission (also added into collision count)
dot3StatsExcessiveCollisions	(Not supported by E-Series or G-Series) Number of frames where transmissions failed because of excessive collisions
dot3StatsCarrierSenseErrors	(G-Series only) The number of transmission errors on a particular interface that are not otherwise counted
dot3StatsSQETestErrors	(G-Series only) A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address; this does not include multicast packets
etherStatsCollisions	An estimate of the total number of collisions on this Ethernet segment. The value returned depends on the location of the RMON probe. Section 8.2.1.3 (10Base5) and Section 10.3.1.3 (10Base2) of the IEEE 802.3 standard state that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus, a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment. Probe location plays a much smaller role when considering 10BaseT. Section 14.2.1.4 (10BaseT) of the IEEE 802.3 standard defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BaseT station can only detect collisions when it is transmitting. Thus, probes placed on a station and a repeater should report the same number of collisions. An RMON probe inside a repeater should report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.
etherStatsCollisionFrames	An estimate of the total number of collisions on this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10Base5) and Section 10.3.1.3 (10Base2) of the IEEE 802.3 standard state that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus, a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment.

	Probe location plays a much smaller role when considering 10BaseT. Section 14.2.1.4 (10BASE-T) of the IEEE 802.3 standard defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BaseT station can only detect collisions when it is transmitting. Thus, probes placed on a station and a repeater, should report the same number of collisions. An RMON probe inside a repeater should report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.
etherStatsDropEvents	The total number of events in which packets were dropped by the probe due to lack of resources. This number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
etherStatsJabbers	Total number of octets of data (including bad packets) received on the network
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
etherStatsUndersizePkts	Number of packets received with a length less than 64 octets
etherStatsFragments	Total number of packets that are not an integral number of octets or have a bad FCS, and that are less than 64 octets long
etherStatsPkts64Octets	Total number of packets received (including error packets) that were 64 octets in length
etherStatsPkts65to127Octets	Total number of packets received (including error packets) that were 65 to 172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 to 255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 to 511 octets in length
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 to 1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 to 1518 octets in length
etherStatsJabbers	Total number of packets longer than 1518 octets that were not an integral number of octets or had a bad FCS
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets
etherStatsCollisions	Best estimate of the total number of collisions on this segment

Table 22-6: Ethernet Threshold Variables (MIBs)

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

Table 22-7: POS Threshold Variables (MIBs)

Variable	Definition
ifInPayloadCrcErrors	Number of CRC errors in the frame inside the GFP/HDLC payload coming in from the SONET receive (RX) direction.
ifOutPayloadCrcErrors	Number of CRC errors in the frame inside the GFP/HDLC payload coming in from the SONET transmit (TX) direction
ifOutOversizePkts	Number of packets larger than 1518 bytes sent out into SONET. Packets larger than 1600 bytes do not get transmitted.
etherStatsDropEvents	Number of received frames dropped at the port level.
gfpStatsRxSBitErrors	Receive frames with Single Bit Errors (cHEC, tHEC, eHEC)
gfpStatsRxMBitErrors	Receive frames with Multi Bit Errors (cHEC, tHEC, eHEC)
gfpStatsRxTypeInvalid	Receive frames with invalid type (PTI, EXI, UPI)
gfpStatsRxCRCErrors	Receive data frames with Payload cyclic redundancy check (CRC) errors
gfpStatsRxCIDInvalid	Receive frames with Invalid CID
gfpStatsCSFRaised	Number of receive (Rx) client management frames with Client Signal Fail indication.
gfpStatsRxFrame	Receive data frames
gfpStatsTxFrame	Transmit data frames
gfpStatsRxOctets	Received data Octets
gfpStatsTxOctets	Transmit data Octets

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

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

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

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

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

DLP-A534 Provision OSI Routing Mode

Purpose	This task provisions the Open System Interconnection (OSI) routing mode. Complete this task when the ONS 15454 is connected to networks with third party network elements (NEs) that use the OSI protocol stack for data communications network (DCN) communication.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution! Do not complete this task until you confirm the role of the node within the network. It will be either an ES, IS Level 1, or IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*.

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

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

Note: For ONS 15454 nodes, three virtual routers can be provisioned. The node primary NSAP address is also the Router 1 primary manual area address. To edit the primary NSAP, you must edit the Router 1 primary manual area address. After you enable Router 1 on the Routers subtab, the Change Primary Area Address button is available to edit the address.

1. Complete the "DLP-A60 Log into CTC" task at the node where you want to provision the OSI

routing mode. If you are already logged in, continue with Step 2.

2. In node view, click the **Provisioning > OSI > Main Setup** tabs.
3. Choose a routing mode:

- End System-The ONS 15454 performs OSI end system (ES) functions and relies upon an intermediate system (IS) for communication with nodes that reside within its OSI area.
  Note: The End System routing mode is not available if more than one virtual router is enabled.
- Intermediate System Level 1-The ONS 15454 performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.
- Intermediate System Level 1/Level 2-The ONS 15454 performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. Before choosing this option, verify the following:
  - ◊ The node is connected to another IS Level 1/Level 2 node that resides in a different OSI area.
  - ◊ The node is connected to all nodes within its area that are provisioned as IS L1/L2.

4. If needed, change the LSP data buffers:

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

5. Return to your originating procedure (NTP).

DLP-A535 Provision or Modify TARP Operating Parameters

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

1. In node view, click the **Provisioning > OSI > TARP > Config** tabs.
2. Provision the following parameters, as needed:

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

NE from which the PDU was received.
Note: The TARP PDUs L1 Propagation parameter is not used when the Node Routing Area (Provisioning > OSI > Main Setup tab) is set to End System.

- TARP PDUs L2 Propagation-If checked (default), TARP Type 2 PDUs received by the node that are not excluded by the LDB are propagated to other NEs within the Level 2 OSI areas. (Type 2 PDUs request a protocol address that matches a TID within a Level 2 routing area.) The propagation occurs if the NE is not the target of the Type 2 PDU, and PDUs are not propagated to the NE from which the PDU was received.
  Note: The TARP PDUs L2 Propagation parameter is only used when the Node Routing Area is provisioned to Intermediate System Level 1/Level 2.
- TARP PDUs Origination-If checked (default), the node performs all TARP origination functions including:
  - ◊ TID to Network Service Access Point (NSAP) resolution requests (originate TARP Type 1 and Type 2 PDUs)
  - ◊ NSAP to TID requests (originate Type 5 PDUs)
  - ◊ TARP address changes (originate Type 4 PDUs)

  Note: TARP Echo and NSAP to TID is not supported.
- TARP Data Cache-If checked (default), the node maintains a TARP data cache (TDC). The TDC is a database of TID to NSAP pairs created from TARP Type 3 PDUs received by the node and modified by TARP Type 4 PDUs (TID to NSAP updates or corrections). TARP 3 PDUs are responses to Type 1 and Type 2 PDUs. The TDC can also be populated with static entries entered on the TARP > Static TDC tab.
  Note: This parameter is only used when the TARP PDUs Origination parameter is enabled.
- L2 TARP Data Cache-If checked (default), the TIDs and NSAPs of NEs originating Type 2 requests are added to the TDC before the node propagates the requests to other NEs.

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

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

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

- LAN TARP Storm Suppression-If checked (default), enables TARP storm suppression. This function prevents redundant TARP PDUs from being unnecessarily propagated across the LAN network.
- Send Type 4 PDU on Startup-If checked, a TARP Type 4 PDU is originated during the initial ONS 15454 startup. Type 4 PDUs indicate that a TID or NSAP change has occurred at the NE. (The default setting is not enabled.)
- Type 4 PDU Delay-Sets the amount of time that will pass before the Type 4 PDU is generated when Send Type 4 PDU on Startup is enabled. 60 seconds is the default. The range is 0 to 255 seconds.
  Note: The Send Type 4 PDU on Startup and Type 4 PDU Delay parameters are not used if TARP PDUs Origination is not enabled.
- LDB Entry-Sets the TARP loop detection buffer timer. The LDB buffer time is assigned to each LDB entry for which the TARP sequence number (tar-seq) is zero.

The default is 5 minutes. The range is 1 to 10 minutes.
- LDB Flush-Sets the frequency period for flushing the LDB. The default is 5 minutes. The range is 0 to 1440 minutes.
- T1-Sets the amount of time to wait for a response to a Type 1 PDU. Type 1 PDUs seek a specific NE TID within an OSI Level 1 area. The default is 15 seconds. The range is 0 to 3600 seconds.
- T2-Sets the amount of time to wait for a response to a Type 2 PDU. TARP Type 2 PDUs seek a specific NE TID value within OSI Level 1 and Level 2 areas. The default is 25 seconds. The range is 0 to 3600 seconds.
- T3-Sets the amount of time to wait for an address resolution request. The default is 40 seconds. The range is 0 to 3600 seconds.
- T4-Sets the amount of time to wait for an error recovery. This timer begins after the T2 timer expires without finding the requested NE TID. The default is 20 seconds. The range is 0 to 3600 seconds.
  Note: The T1, T2, and T4 timers are not used if TARP PDUs Origination is not enabled.

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

DLP-A536 Add a Static TID to NSAP Entry to the TARP Data Cache

Purpose	This task adds a static TID to NSAP entry to the TDC. The static entries are required for NEs that do not support TARP and are similar to static routes. For a specific TID, you must force a specific NSAP.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

1. In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.
2. Click **Add Static Entry**.
3. In the Add Static Entry dialog box, enter the following:
   - TID-Enter the TID of the NE. (For ONS nodes, the TID is the Node Name parameter on the node view Provisioning > General tab.)
   - NSAP-Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.
4. Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.
5. Return to your originating procedure (NTP).

DLP-A537 Remove a Static TID to NSAP Entry from the TARP Data Cache

Purpose	This task removes a static TID to NSAP entry from the TDC.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

1. In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.
2. Click the static entry that you want to delete.
3. Click **Delete Static Entry**.
4. In the Delete TDC Entry dialog box, click **Yes**.
5. Return to your originating procedure (NTP).

DLP-A538 Add a TARP Manual Adjacency Table Entry

Purpose	This task adds an entry to the TARP manual adjacency table (MAT). Entries are added to the MAT when the ONS 15454 must communicate across routers or non-SONET NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In the node view, click the **Provisioning > OSI > TARP > MAT** tabs.
2. Click **Add**.
3. In the Add TARP Manual Adjacency Table Entry dialog box, enter the following:
   - Level-Sets the TARP Type Code that will be sent:
     - **Level 1**-Indicates that the adjacency is within the same area as the current node. The entry generates Type 1 PDUs.
     - **Level 2**-Indicates that the adjacency is in a different area than the current node. The entry generates Type 2 PDUs.
   - NSAP-Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.
4. Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.
5. Return to your originating procedure (NTP).

DLP-A539 Provision OSI Routers

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

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

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

Note: The System ID for Router 1 is the node MAC address. The System IDs for Routers 2 and 3 are created by adding 1 and 2 respectively to the Router 1 System ID. You cannot edit the System IDs.

1. In node view, click the **Provisioning > OSI > Routers > Setup** tabs.
2. Chose the router you want provision and click **Edit**. The OSI Router Editor dialog box appears.
3. In the OSI Router Editor dialog box:
    1. Check **Enable Router** to enable the router and make its primary area address available for editing.
    2. Click the manual area address, then click **Edit**.
    3. In the Edit Manual Area Address dialog box, edit the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the edits in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 8 to 24 alphanumeric characters (0-9, a-f) in length.
    4. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Edit Manual Area Address, and OSI Router Editor.
4. Return to your originating procedure (NTP).

DLP-A540 Provision Additional Manual Area Addresses

Purpose	This task provisions the OSI manual area addresses. One primary and two additional manual areas can be created for each virtual router.
Tools/Equipment	None
Prerequisite Procedures	DLP-A539 Provision OSI Routers DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > OSI > Routers > Setup** tabs.
2. Chose the router where you want provision an additional manual area address and click **Edit**. The OSI Router Editor dialog box.
3. In the OSI Router Editor dialog box:
    1. Check **Enable Router** to enable the router and make its primary area address available for editing.
    2. Click the manual area address, then click **Add**.
    3. In the Add Manual Area Address dialog box, enter the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 2 to 24 alphanumeric characters (0-9, a-f) in length.
    4. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Add Manual Area Address, and OSI Router Editor.
4. Return to your originating procedure (NTP).

DLP-A541 Enable the OSI Subnet on the LAN Interface

Purpose	This task enables the OSI subnetwork point of attachment on the LAN interface.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: OSI subnetwork points of attachment are enabled on DCCs when you create DCCs. See the "DLP-A377 Provision Section DCC Terminations" task and the "DLP-A378 Provision Line DCC Terminations" task.

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

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

1. In node view, click the **Provisioning > OSI > Routers > Subnet** tabs.
2. Click **Enable LAN Subnet**.
3. In the Enable LAN Subnet dialog box, complete the following fields:
   - ESH-Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
   - ISH-Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
   - IIH-Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
   - IS-IS Cost-Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default IS-IS cost for LAN subnets is 20. It normally should not be changed.
   - DIS Priority-Sets the designated intermediate system (DIS) priority. In IS-IS networks, one router is elected to serve as the DIS (LAN subnets only). Cisco router DIS priority is 64. For the ONS 15454 LAN subnet, the default DIS priority is 63. It normally should not be changed.
4. Click **OK**.
5. Return to your originating procedure (NTP).

DLP-A542 Create an IP-Over-CLNS Tunnel

Purpose	This task creates an IP-over-CLNS tunnel to allow ONS 15454s to communicate across equipment and networks that use the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution! IP-over-CLNS tunnels require two end points. You will create one point on an ONS 15454. The other end point is generally provisioned on non-ONS equipment including routers and other network elements (NE). Before you begin, verify that you have the capability to create an OSI over IP tunnel on the other equipment location.

1. In node view, click the **Provisioning > OSI > Tunnels** tabs.
2. Click **Create**.
3. In the Create IP Over OSI Tunnel dialog box, complete the following fields:

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

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

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

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

4. Click **OK**.
5. Provision the other tunnel end point using the documentation.
6. Return to your originating procedure (NTP).

DLP-A543 Remove a TARP Manual Adjacency Table Entry

Purpose	This task removes an entry from the TARP manual adjacency table.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

1. In node view, click the **Provisioning > OSI > TARP > MAT** tabs.
2. Click the MAT entry that you want to delete.
3. Click **Remove**.
4. In the Delete TDC Entry dialog box, click **OK**.
5. Return to your originating procedure (NTP).

DLP-A544 Change the OSI Routing Mode

Purpose	This task changes the OSI routing mode.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution! Do not complete this procedure until you confirm the role of the node within the network. It will be either an ES, IS Level 1, or IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*.

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

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

1. Verify the following:
   - All L1/L2 virtual routers on the NE must reside in the same area. This means that all neighboring virtual routers must have at least one common area address.
   - For OSI L1/L2 to ES routing mode changes, only one L1/L2 virtual router and no more than one subnet can be configured.
   - For OSI L1 to ES routing mode changes, only one L1 virtual router and no more than one subnet can be configured.
2. In node view, click the **Provisioning > OSI** tabs.
3. Choose one of the following routing modes:

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

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

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

   - L1 LSP Buffer Size-Adjusts the Level 1 link state PDU buffer size.
   - L2 LSP Buffer Size-Adjusts the Level 2 link state PDU buffer size.
5. Return to your originating procedure (NTP).

DLP-A545 Edit the OSI Router Configuration

Purpose	This task allows you to edit the OSI router configuration, including enabling and disabling OSI routers, editing the primary area address, and creating or editing additional area addresses.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC

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

1. In node view, click the **Provisioning > OSI > Routers > Setup** tabs.
2. Chose the router you want provision and click **Edit**.
3. In the OSI Router Editor dialog box:
    1. Check or uncheck the Enabled box to enable or disable the router.
        Note: Router 1 must be enabled before you can enable Routers 2 and 3.
    2. For enabled routers, edit the primary area address, if needed. The address can be between 8 and 24 alphanumeric characters in length.
    3. If you want to add or edit an area address to the primary area, enter the address at the bottom of the Multiple Area Addresses area. The area address can be 2 to 26 numeric characters (0-9) in length. Click **Add**.
    4. Click **OK**.
4. Return to your originating procedure (NTP).

DLP-A546 Edit the OSI Subnetwork Point of Attachment

Purpose	This task allows you to view and edit the OSI subnetwork point of attachment parameters. The parameters are initially provisioned when you create a Section DCC (SDCC), Line DCC (LDCC), generic communications channel (GCC), or optical service channel (OSC), or when you enable the LAN subnet.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > OSI > Routers > Subnet** tabs.
2. Choose the subnet you want to edit, then click **Edit**.
3. In the Edit <*subnet type*> Subnet <*slot/port*> dialog box, edit the following fields:
    - ESH-The End System Hello PDU propagation frequency. An end system NE transmits ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
    - ISH-The Intermediate System Hello PDU propagation frequency. An intermediate system NE sends ISHs to other ESs and ISs to inform them about the NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
    - IIH-The Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
      Note: The IS-IS Cost and DIS Priority parameters are provisioned when you create or enable a subnet. You cannot change the parameters after the subnet is created. To change the DIS Priority and IS-IS Cost parameters, delete the subnet and create a new one.

3. Click **OK**.
4. Return to your originating procedure (NTP).

DLP-A547 Edit an IP-Over-CLNS Tunnel

Purpose	This task allows you to edit the parameters of an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-A542 Create an IP-Over-CLNS Tunnel DLP-A60 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

1. In node view, click the **Provisioning > OSI > Tunnels** tabs.
2. Click **Edit**.
3. In the Edit IP Over OSI Tunnel dialog box, complete the following fields:

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

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

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

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

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

DLP-A548 Delete an IP-Over-CLNS Tunnel

Purpose	This task allows you to delete an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

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

1. In node view, click the **Provisioning > OSI > Tunnels** tabs.
2. Choose the IP-over-CLNS tunnel that you want to delete.
3. Click **Delete**.
4. Click **OK**.
5. Return to your originating procedure (NTP).

DLP-A549 View IS-IS Routing Information Base

Purpose	This task allows you to view the Intermediate System to Intermediate System (IS-IS) protocol routing information base (RIB). IS-IS is an OSI routing protocol that floods the network with information about NEs on the network. Each NE uses the information to build a complete and consistent picture of a network topology. The IS-IS RIB shows the network view from the perspective of the IS node.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In the node view, click the **Maintenance > OSI > IS-IS RIB** tabs.
2. View the following RIB information for Router 1:
   - Subnet Type-Indicates the OSI subnetwork point of attachment type used to access the destination address. Subnet types include SDCC, LDCC, GCC, OSC, and LAN.
   - Location-Indicates the OSI subnetwork point of attachment. For DCC subnets, the slot and port are displayed. LAN subnets are shown as LAN.
   - Destination Address-The destination NSAP (network service access point) of the IS.
   - MAC Address-For destination NEs that are accessed by LAN subnets, the NE's Media Access Control address.
3. If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.
4. Return to your originating procedure (NTP).

DLP-A550 View ES-IS Routing Information Base

Purpose	This task allows you to view the End System to Intermediate System (ES-IS) protocol routing information base (RIB). ES-IS is an OSI protocol that defines how end systems (hosts) and intermediate systems (routers) learn about each other. For ESs, the ES-IS RIB shows the network view from the perspective of the ES node. For ISs, the ES-IS RIB shows the network view from the perspective of the IS node.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
	As needed

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

1. In node view, click the **Maintenance > OSI > ES-IS RIB** tabs.
2. View the following RIB information for Router 1:
   - Subnet Type-Indicates the OSI subnetwork point of attachment type used to access the destination address. Subnet types include SDCC, LDCC, GCC, OSC, and LAN.
   - Location-Indicates the subnet interface. For DCC subnets, the slot and port are displayed. LAN subnets are shown as LAN.
   - Destination Address-The destination IS NSAP (network service access point).
   - MAC Address-For destination NEs that are accessed by LAN subnets, the NE's Media Access Control address.
3. If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.
4. Return to your originating procedure (NTP).

DLP-A551 Manage the TARP Data Cache

Purpose	This task allows you to view and manage the TARP data cache (TDC). The TDC facilitates TARP processing by storing a list of TID to NSAP mappings.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Maintenance > OSI > TDC** tabs.
2. View the following TARP data cache information:
   - TID-The target identifier of the originating NE. For ONS 15454s, the TID is the name entered in the Node Name/TID field on the Provisioning > General tab.
   - NSAP/NET-The Network Service Access Point or Network Element Title of the originating NE.
   - Type-Indicates how the TARP data cache entry was created:
     - Dynamic-The entry was created through the TARP propagation process.
     - Static-The entry was manually created and is a static entry.
3. If you want to query the network for an NSAP that matches a TID, complete the following steps. Otherwise, continue with Step 4.

   Note: The TID to NSAP function is not available if the TARP data cache is not enabled on the Provisioning > OSI > TARP subtab.

   1. Click the **TID to NSAP** button.
   2. In the TID to NSAP dialog box, enter the TID you want to map to an NSAP.
   3. Click **OK**, then click **OK** on the information message.
   4. On the TDC tab, click **Refresh**.
      If TARP finds the TID in its TDC it returns the matching NSAP. If not, TARP sends PDUs across the network. Replies will return to the TDC later, and a check TDC later message is displayed.
4. If you want to delete all the dynamically-generated TDC entries, click the **Flush Dynamic Entries** button. If not, continue with Step 5.

5. Return to your originating procedure (NTP).

DLP-A552 Adjust the Java Virtual Memory Heap Size

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

1. Click Start > Settings > Control Panel. The Windows Control Panel appears.
2. Double-click System. The System Properties window appears.
3. Click the Advanced tab.
4. Click Environmental Variables. The Environmental Variables window appears.
5. In the User Variables area, click New. The New User Variable window appears.
6. Type **CTC_HEAP** in the Variable Name field.
7. Type **512** in the Variable Value field.
8. Click OK.
9. Reboot your PC.
10. Return to your originating procedure (NTP).

DLP-A553 Upgrade DS1 or DS3-12 Cards in a 1:N or 1:1 Configuration to High-Density Electrical Cards

Purpose	This task upgrades low-density electrical cards in a 1:N protection scheme (where N = 1 or 2) to high-density electrical cards (DS3/EC1-48, DS1/E1-56). Low-density cards are defined as DS-1 and DS3-12.
Tools/Equipment	DS3/EC1-48 card(s), as needed DS1/E1-56 card(s), as needed High-density shelf assembly (15454-SA-HD) High-density EIA (MiniBNC, UBIC-V, UBIC-H) installed.
Prerequisite Procedures	NTP-A17 Install the Electrical Cards
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

1. Complete the "DLP-A60 Log into CTC" task. If you are already logged in, continue with Step 2.
2. According to local site practice, complete the "NTP-A108 Back Up the Database" procedure.
3. Determine which low-density card(s) (DS-1, DS-3, DS-3E) you want to upgrade to high-density, according to slot limitations.

Note: For 1:N protection groups, the protect card is installed in Slot 3 on the A side of the shelf and Slot 15 on the B side. For 1:1 protect groups, working and protect cards can be installed in any traffic slot.

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

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

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

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

4. In node view, double-click the current protect card. The card view appears.
5. Make sure the current protect card is not active:
    1. In card view, click the Maintenance > Protection tabs.
    2. Select the protection group where the protect card resides.
6. If the card status is Protect/Active, perform a switch so that the protect card becomes standby:
    1. Click Switch.
    2. Click Yes in the confirmation dialog box.
7. Physically remove the card.
    1. Open the card ejectors.
    2. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.
8. Right-click the Protect/Standby slot and change the low-density card to the high-density card:
    1. Choose Change Card from the drop-down list.
    2. Choose the new high-density card type from the Change to drop-down list.
    3. Click OK.
9. Physically insert the new high-density electrical card into the protect slot. Be sure to remove the plastic protective covers on rear of the card before installing the card.
    1. Open the ejectors on the card.
    2. Slide the card into the slot along the guide rails.
    3. Close the ejectors.

    Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during the high-density card boot-up, see the "NTP-A17 Install the Electrical Cards" procedure.

10. Because the low-density working card is now active, switch traffic away from the low-density card:
    1. In node view, double-click the slot where the low-density card is installed.
    2. Click the Maintenance > Protection tabs.
    3. Double-click the protection group that contains the working card.
    4. Click the low-density card slot.
    5. Click Switch and Yes in the Confirmation dialog box.
11. Physically remove the low-density card you switched traffic away from in Step 10:
    1. Open the card ejectors.
    2. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.
12. Change the low-density card to the high-density card in CTC:
    1. Right-click the slot where you removed the low-density card and choose Change Card from the drop-down list
    2. Choose the new card type from the Change to drop-down list
    3. Click OK.
13. Insert the new high-density electrical card into the slot where you removed the low-density card. Be sure to remove the plastic protective covers on rear of the card before installing the card:
    1. Open the ejectors on the card.
    2. Slide the card into the slot along the guide rails.
    3. Close the ejectors.

    Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during high-density electrical card bootup, see the "NTP-A17 Install the Electrical Cards" procedure.

14. Clear the switch you performed in Step 10:
    1. In node view, double-click the slot where you installed the high-density card in Step 13.
    2. In the Maintenance > Protection tab, double-click the protection group that contains the reporting card.
    3. Click the selected group.
    4. Click Switch and click Yes in the confirmation dialog box.
    5. The protect card should now become standby.
15. If you have upgraded to a DS3/EC1-48 card and are using 734A cables with UBIC electrical interface adapters (EIAs), you must set the LBO for Ports 13 to 48 (DS3/EC1-48), doing so according to the actual distance (in feet) from the LBX panel.

    If you are using 735A cables, you must set the LBO for Ports 13 to 48 (DS3/EC1-48), doing so according to the following conventions:

    · Actual distance from the DSX panel is less than 110 feet (33.53 m):
    LBO setting is " 0 - 225."
    · Actual distance from the DSX panel is greater than or equal to 110 feet (33.53 m):
    LBO setting is "226 to 450."

    If you have upgraded to a DS1/E1-56 card with UBIC EIAs, you must set the LBO for Ports 15 to 56, doing so according to the actual distance (in feet) from the LBX panel. Repeat Steps 4 through 14 for any other low-density cards you want to upgrade to high-density cards.

16. Return to your originating procedure (NTP).

DLP-A553 Upgrade DS3XM-6 Cards in a 1:1 Configuration to High-Density DS3XM-12 Electrical Cards

Purpose	This task upgrades low-density electrical cards in a 1:1 protection scheme to

	high-density electrical cards (DS3XM-12 cards). This procedure upgrades low-density DS3XM-6 cards in a 1:1 protection scheme to high-density DS3XM-12 cards.
Tools/Equipment	DS3XM-12 card(s), as needed. Upgrade of DS3XM-6 to DS3XM-12 does not require a High-density shelf assembly. The upgrade can be performed on low-density shelf assembly as well.
Prerequisite Procedures	NTP-A17 Install the Electrical Cards
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note: You cannot have any DS-1 cards installed on the same side of the shelf as the DS3XM-12 card when you finish the low-density to high-density upgrade.

Caution! After upgrading a DS3XM-6 card to a DS3XM-12 card, the newly installed DS3XM-12 card will run in STS-12 mode. To change the backplane throughput rate, make sure the card is out-of-service and not carrying live traffic. Changing the backplane throughput rate on a in-service card can cause a traffic outage of up to 50 ms.

1. Complete the "DLP-A60 Log into CTC" task on page 17-68. If you are already logged in, continue with Step 2.
2. According to local site practice, complete the "NTP-A108 Back Up the Database" procedure.
3. Determine which low-density card(s) (DS3XM-6) you want to upgrade to high-density, according to slot limitations.

   Note: For 1:1 protect groups, working and protect cards can be installed in any traffic slot. But both cards should be placed adjacent to each other.

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

   - The protect card must be in a protection group.
   - For 1:N protection groups where N = 1: If 1:1 is created on A side protect card cannot be upgraded if an DS1 card is installed or preprovisioned in A side. If 1:1 is created On the B side the protect card cannot be DS1 card is installed or preprovisioned in B side

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

   - A working card on the A cannot be upgraded if an DS1 card is installed or preprovisioned in A side.
   - A working card on the B side cannot be upgraded if an DS1 card is installed or preprovisioned in B side.

4. In node view, double-click the current protect card. The card view appears.
5. Make sure the current protect card is not active:
   1. In card view, click the Maintenance > Protection tabs.
   2. Select the protection group where the protect card resides.
6. If the card status is Protect/Active, perform a switch so that the protect card becomes standby:
   1. Click Switch.
   2. Click Yes in the confirmation dialog box.

7. Physically remove the card:
    1. Open the card ejectors.
    2. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.
8. Right-click the Protect/Standby slot and change the low-density card to the high-density card:
    1. Choose Change Card from the drop-down list.
    2. Choose the new high-density card type from the Change to drop-down list.
    3. Click OK.
9. Physically insert the new high-density electrical card into the protect slot. Be sure to remove the plastic protective covers on rear of the card before installing the card.
    1. Open the ejectors on the card.
    2. Slide the card into the slot along the guide rails.
    3. Close the ejectors.

    Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during the high-density card boot-up, see the "NTP-A17 Install the Electrical Cards" procedure.

10. Because the low-density working card is now active, switch traffic away from the low-density card:
    1. In node view, double-click the slot where the low-density card is installed.
    2. Click the Maintenance > Protection tabs.
    3. Double-click the protection group that contains the working card.
    4. Click the low-density card slot.
    5. Click Switch and Yes in the Confirmation dialog box.
11. Physically remove the low-density card you switched traffic away from in Step 10:
    1. Open the card ejectors.
    2. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.
12. Change the low-density card to the high-density card in CTC:
    1. Right-click the slot where you removed the low-density card and choose Change Card from the drop-down list.
    2. Choose the new high-density card type from the Change to drop-down list.
    3. Click OK.
13. Insert the new high-density electrical card into the slot where you removed the low-density card. Be sure to remove the plastic protective covers on rear of the card before installing the card:
    1. Open the ejectors on the card.
    2. Slide the card into the slot along the guide rails.
    3. Close the ejectors.

    Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during high-density electrical card bootup, see the "NTP-A17 Install the Electrical Cards" procedure.

14. Clear the switch you performed in Step 10:
    1. In node view, double-click the slot where you installed the high-density card in Step 13.
    2. In the Maintenance > Protection tab, double-click the protection group that contains the reporting card.
    3. Click the selected group.
    4. Click Switch and Click Yes in the confirmation dialog box.

    The protect card should now become standby.

    Note: After upgrading a DS3XM-6 card to a DS3XM-12 card, the newly installed DS3XM-12 card will run in STS-12 mode. Go to CTC Card View/Maintenance/Card window to change Backplane Throughput bandwidth to STS48 and refresh viewer window.

If you want to create 1:N on DS3XM-12 cards only slot numbers 3 and 15 should be listed for protect card selection.

15. If you have upgraded to a DS3XM-12 and are using 734A cables with UBIC electrical interface adapters (EIAs), you must set the LBO for Ports 7 to 12 (DS3XM-12doing so according to the actual distance (in feet) from the LBX panel.

    If you are using 735A cables, you must set the LBO for Ports 7 to 12 (DS3XM-12doing so according to the following conventions:

    Actual distance from the DSX panel is less than 110 feet (33.53 m):

    LBO setting is " 0 - 225."

    Actual distance from the DSX panel is greater than or equal to 110 feet (33.53 m):

    LBO setting is "226 to 450."

16. Return to your originating procedure (NTP).

DLP-A554 Upgrade EC-1 Cards in a 1:1 Configuration to DS3/EC1-48 Cards

Purpose	This task upgrades low-density electrical cards in a 1:N protection scheme (where N = 1 or 2) to high-density electrical cards (DS3/EC1-48, DS1/E1-56, and DS3XM-12 cards). Low-density cards are defined as DS-1 and DS3-12. This procedure also upgrades low-density electrical cards (DS3XM-6 cards) in a 1:1 protection scheme to high-density electrical cards (DS3XM-12 cards).
Tools/Equipment	DS3/EC1-48 card(s), as needed DS3XM-12 card(s), as needed DS1/E1-56 card(s), as needed High-density shelf assembly (15454-SA-HD) High-density EIA (MiniBNC, UBIC-V, UBIC-H) installed
Prerequisite Procedures	NTP-A17 Install the Electrical Cards
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Caution! After upgrading a DS3XM-6 card to a DS3XM-12 card, the newly installed DS3XM-12 card will run in STS-12 mode. To change the backplane throughput rate, make sure the card is out-of-service and not carrying live traffic. Changing the backplane throughput rate on a in-service cardcan cause a traffic outage of up to 50 ms.

1. Complete the DLP-A60 Log into CTC. If you are already logged in, continue with Step 2.

2. According to local site practice, complete the NTP-A108 Back Up the Database.
3. Determine which low-density card(s) you want to upgrade to high-density, according to slot limitations.

   Note: For 1:N protection groups, the protect card is installed in Slot 3 on the A side of the shelf and Slot 15 on the B side. For 1:1 protect groups, working and protect cards can be installed in any traffic slot.

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

   - If you are upgrading an EC1-12 card in a 1:1 protection group to a DS3/EC1-48 card, the EC1-12 cards must be in either Slots 1 and 2 or 16 and 17.
   - If you are upgrading EC1-12 cards in a 1:1 protection group to a DS3/EC1-48 card, Slot 3 needs to be unoccupied if upgrading on the A-Side, and Slot 15 needs to be unoccupied if upgrading on the B-Side.
4. In node view, double-click the current protect card. The card view appears.

   Slot 1 contains the protect card if you are working on the A side of the shelf, and Slot 17 contains the protect card if you are working on the B side of the shelf.
5. Make sure the current protect card is not active:
   1. In card view, click the **Maintenance > Protection** tabs.
   2. Select the protection group where the protect card resides.
6. If the card status is Protect/Active, perform a switch so that the protect card becomes standby:
   1. Click **Switch**.
   2. Click **Yes** in the confirmation dialog box.
7. Physically insert the new high-density electrical card into the new 1:N protect slot (Slot 3 for the A-Side and Slot 15 for the B-Side). Be sure to remove the plastic protective covers on rear of the card before installing the card.
   1. Open the ejectors on the card.
   2. Slide the card into the slot along the guide rails.
   3. Close the ejectors.

      For more information about LED behavior during the high-density card boot-up, see theNTP-A17 Install the Electrical Cards. Allow the card to completely boot up before proceeding.
8. Delete the 1:1 EC1-12 low density protection group. See the "DLP-A155 Delete a Protection Group" task.
   1. Open the card ejectors.
   2. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.
9. Create a 1:N protection group for the EC1-12 cards and the new DS3/EC1-48 card. See the "NTP-A324 Create Protection Groups" task.

   Note: Make sure that the new protection group is 1:N and not 1:1. If you upgrading the A side of the shelf, make sure the protect card is in Slot 3 and the working cards are Slots 1 and 2. If you are upgrading the B side of the shelf, make sure the protect card is in Slot 15 and the working cards are in Slots 16 and 17.
10. Because the low-density card is now active, switch traffic away from the low-density card in Slot 1 if you are working on the A side, or Slot 17 if you are working on the B side:
    1. In node view, double-click the card in Slot 1/Slot 17.
    2. Click the **Maintenance > Protection** tabs.
    3. Double-click the protection group that contains the working card in Slot 1/Slot 17.
    4. Click the card in Slot 1/Slot 17.
    5. Click **Switch** and **Yes** in the Confirmation dialog box.
11. Physically remove the low-density card in Slot 1/Slot 17:
    1. Open the card ejectors.
    2. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.
12. Change the low-density card to the high-density card in CTC:

   1. Right-click Slot 1/Slot 17 and choose **Change Card** from the drop-down list.
   2. Choose the new card type from the Change to drop-down list.
   3. Click **OK**.
13. Insert the new high-density electrical card into Slot 1/Slot 17. Be sure to remove the plastic protective covers on rear of the card before installing the card:
   1. Open the ejectors on the card.
   2. Slide the card into the slot along the guide rails.
   3. Close the ejectors.
      Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during the high-density card bootup, see the NTP-A17 Install the Electrical Cards.
14. Clear the switch you performed in Step 10:
   1. In node view, double-click the card in Slot 1/Slot 17.
   2. In the Maintenance > Protection tab, double-click the protection group that contains the reporting card.
   3. Click the selected group.
   4. Click **Clear** and click **Yes** in the confirmation dialog box.
      The protect card in Slot 3 (A side) or Slot 15 (B side) should now become standby.
      Note: If you have upgraded to a DS3/EC1-48 card and are using 734A cables with UBIC electrical interface adapters (EIAs), you must set the LBO for Ports 13 to 48, doing so according to the actual distance (in feet) from the LBX panel. If you are using 735A cables, you must set the LBO for Ports 13 to 48, doing so according to the following conventions:

      ◊ Actual distance from the DSX panel is less than 110 feet (33.53 m):
        LBO setting is " 0 - 225."
      ◊ Actual distance from the DSX panel is greater than or equal to 110 feet (33.53 m):
        LBO setting is "226 to 450."

15. As necessary, repeat Steps 4 through 14 for other low-density electrical cards you want to upgrade.
16. Return to your originating procedure (NTP).

DLP-A555 Set Up SDH External or Line Timing

Purpose	This task defines the SDH timing source (external or line) for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > Timing** > General tabs.
2. In the Timing Standard area, make sure that the Current Timing Standard is SDH. If it is not, continue with Step 3. If the Current Timing Standard is SDH, skip to Step 4.
3. Click Change to switch the timing from SONET to SDH.
   Note: Changing the timing standard reinitializes the node and might affect traffic.
4. In the General Timing area, complete the following information:
   ♦ Timing Mode-Choose **External** if the ONS 15454 derives its timing from a BITS source wired to the backplane pins; choose **Line** if timing is derived from an OC-N card that is optically connected to the timing node. A third option, Mixed, allows you to set external and

line timing references.

Note: Because Mixed timing might cause timing loops, Cisco does not recommend its use. Use this mode with care.

- Revertive-Select this check box if you want the ONS 15454 to revert to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- Reversion Time-If Revertive is checked, choose the amount of time that the ONS 15454 will wait before reverting to its primary timing source. Five minutes is the default.

5. In the Reference Lists area, complete the following information:

   Note: You can define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out pins on the backplane. If you attach equipment to BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

   - NE Reference-Allows you to define three timing references (Ref 1, Ref 2, Ref 3). The node uses Reference 1 unless a failure occurs to that reference, in which case the node uses Reference 2. If Reference 2 fails, the node uses Reference 3, which is typically set to Internal Clock. The internal clock is the Synchronous Equipment Timing Source (SETS) clock provided on the TCC2/TCC2P card. The options that appear depend on the Timing Mode setting.
   - If the Timing Mode is set to External, your options are BITS1, BITS2, and Internal Clock.
   - If the Timing Mode is set to Line, your options are the node's working OC-N cards and the Internal Clock. Choose the cards/ports that are directly or indirectly connected to the node wired to the BITS source, that is, the node's trunk (span) cards. Set Reference 1 to the trunk card that is closest to the BITS source. For example, if Slot 5 is connected to the node wired to the BITS source, choose Slot 5 as Reference 1.
   - If the Timing Mode is set to Mixed, both BITS and OC-N cards are available, allowing you to set a mixture of external BITS and OC-N trunk (span) cards as timing references.
   - BITS-1 Out/BITS-2 Out-Define the timing references for equipment wired to the BITS Out pins on the backplane. BITS-1 Out and BITS-2 Out are enabled when BITS-1 and BITS-2 facilities are put in service. If Timing Mode is set to External, choose the OC-N card used to set the timing. If Timing Mode is set to Line, you can choose an OC-N card or choose NE Reference to have the BITS-1 Out and/or BITS-2 Out follow the same timing references as the NE.

6. Click the **BITS Facilities** subtab.

   The BITS Facilities section sets the parameters for your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

7. In the BITS In area, complete the following information:
   - Facility Type-For TCC2 and TCC2P cards, choose the BITS signal type supported by your BITS clock, either E1 or 2 MHz. For the TCC2P card only, you can also choose 64 Khz.
   - BITS In State-If Timing Mode is set to External or Mixed, set the BITS In State for BITS-1 and/or BITS-2 to **IS** (in service), depending on whether one or both BITS input pin pairs on the TCC2/TCC2P card are connected to the external timing source. If Timing Mode is set to Line, set the BITS In State to **OOS** (out of service).

8. If BITS In State is set to OOS, continue with Step 9. If the BITS In State is set to IS, complete the following information:
   - Coding-Choose the coding used by your BITS reference, either HDB3 (high-density bipolar order 3) or AMI (alternate mark inversion).
   - Framing-Choose the framing used by your BITS reference, either Unframed, FAS (frame alignment signal), FAS+CAS (frame alignment signal plus channel associated signal), FAS+CRC (frame alignment signal plus cyclic redundancy check), or FAS+CAS+CRC

(frame alignment signal plus channel associated signal plus cyclic redundancy check).
- Sync Messaging-Check this check box to enable SSM. SSM is not available if Framing is set to Unframed, FAS, or FAS+CAS.
- Admin SSM-If the Sync Messaging check box is not checked, you can choose the SSM type from the drop-down list.
- Sa Bit-Choose the Sa bit in the E1 stream to use for incoming SSM messaging, either bit 4, 5, 6, 7, or 8.

9. In the BITS Out area, complete the following information, as needed:
   - Facility Type-(Display only) If the BITS IN signal is E1, the only supported BITS OUT is E1; likewise, if the BITS In signal is 2 MHz, the only supported BITS OUT is 2 MHz.
   - BITS Out State-If equipment is connected to the node's BITS output pins on the backplane and you want to time the equipment from a node reference, set the BITS Out State for BITS-1 and/or BITS-2 to **IS**, depending on which BITS Out pins are used for the external equipment. If equipment is not attached to the BITS output pins, set the BITS Out State to **OOS**.
10. If the BITS Out State is set to OOS, continue with Step 11. If BITS Out State is set to IS, complete the following information:
    - Coding-(Display only) The coding is the same as that selected in the BITS In area.
    - Framing-(Display only) The framing is the same as that selected in the BITS In area.
    - AIS Threshold-If SSM is disabled or Unframed, FAS, or FAS+CAS are used, choose the quality level where a node sends an alarm indication signal (AIS) from the BITS 1 Out and BITS 2 Out backplane pins. An AIS alarm is raised when the optical source for the BITS reference falls to or below the SSM quality level defined in this field.
    - Sa Bit-Choose the Sa bit in the E1 stream to use for outgoing SSM messaging, either bit 4, 5, 6, 7, or 8.
11. Click **Apply**.

    Note: Refer to the *Cisco ONS 15454 Troubleshooting Guide* for timing-related alarms.
12. Return to your originating procedure (NTP).

DLP-A556 Provision the Card Mode for ML-Series Ethernet Cards

Purpose	This task provisions the card mode for ML-Series Ethernet cards (ML100T-12, ML1000-2,and ML100X-8)
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 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 ML-Series Ethernet card graphic to open the card.
2. Click the **Provisioning > Card** tabs.
3. For the ML-Series Ethernet card, select an option from the drop-down Mode menu:
   - HDLC-High-level data link control. (Does not support VLAN trunking, which is standard on most Cisco data devices.)
   - GFP-F-Frame-mapped generic framing procedure, a PDU-oriented adaptation mode that maps a client frame into one GFP frame.
   - RPR 802.17-802.17 Resilient Packet Ring, which is IEEE- compliant.

     Note: For more details about the interoperabilty of Optical Networking System (ONS) Ethernet cards, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.
4. Click **Apply**.

5. Return to your originating procedure (NTP).

DLP-A557 View Multirate PM Parameters

Purpose	This task enables you to view PM counts on a multirate card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 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 multirate card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.
3. In the Port drop-down list, click the port 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 Reference Manual*.
6. To monitor another port on a multiport card, choose another port from the Port drop-down list and click **Refresh**.
7. Return to your originating procedure (NTP).

DLP-A558 Provision the Designated SOCKS Servers

Purpose	This task identifies the ONS 15454 SOCKS servers in SOCKS-proxy-enabled networks. Identifying the SOCKS servers reduces the amount of time required to log into a node and have all NEs appear in network view (NE discovery time). The task is recommended when the combined CTC login and NE discovery time is greater than five minutes in networks with SOCKS proxy enabled. Long (or failed) login and NE discovery times can occur in networks that have a high ENE-to-GNE ratio and a low number of ENEs with LAN connectivity.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note: Note: If you cannot log into a network node, complete the "DLP-A60 Log into CTC" task choosing the Disable Network Discovery option. Complete this task, then log in again with network discovery enabled.

Note: To complete this task, you must have either the IP addresses or DNS names of all ONS 15454 nodes in the network with LAN access that have SOCKS proxy enabled.

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

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

1. From the CTC Edit menu, choose **Preferences**.
2. In the Preferences dialog box, click the **SOCKS** tab.
3. In the Designated SOCKS Server field, type the IP address or DNS node name of the first ONS 15454 SOCKS server. The ONS 15454 that you enter must have SOCKS proxy server enabled, and it must have LAN access.
4. Click **Add**. The node is added to the SOCKS server list. If you need to remove a node on the list, click **Remove**.
5. Repeat Steps 3 and 4 to add all qualified ONS 15454s within the network. All ONS nodes that have SOCKS proxy enabled and are connected to the LAN should be added.
6. Click **Check All Servers**. A check is conducted to verify that all nodes can perform as SOCKS servers. If so, a check is placed next to the node IP address or node name in the SOCKS server list. An X placed next to the node indicates one or more of the following:
   - The entry does not correspond to a valid DNS name.
   - The numeric IP address is invalid.
   - The node cannot be reached.
   - The node can be reached, but the SOCKS port cannot be accessed, for example, a firewall problem might exist.
7. Click **Apply**. The list of ONS 15454s, including ones that received an X in Step 6, are added as SOCKS servers.
8. Click **OK** to close the Preferences dialog box.
9. Return to your originating procedure (NTP).

DLP-A559 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-A260 Set Up Computer for CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

1. Insert the Cisco ONS 15454 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 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-A560 Create an Optimized 1+1 Protection Group

Purpose	This task creates an optimized 1+1 protection group for OC3-4, OC3-8, and MRC-2.5G-4 cards (in OC-3 configurations).
Tools/Equipment	Installed OC3-4 cards, OC3-8 cards, MRC-2.5G-4 cards, or preprovisioned slots
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed; consult your network administrator before using this feature.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. Verify that the cards are installed according to the optimized 1+1 requirements specified in Table 4-1.
2. Change the port type from SONET to SDH for each applicable port on the OC3-4, OC3-8, or MRC-2.5G-4 card where you want to provision a 1+1 optimized protection group:
    1. In node view, double-click the applicable card.
    2. Click the **Provisioning > Line** tabs.
    3. In the Type column next to port, choose SDH from the drop-down list and click Apply.
3. In node view, click the **Provisioning > Protection** tabs.
4. In the Protection Groups area, click **Create**.
5. In the Create Protection Group dialog box, enter the following:
    - Name-Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (") characters.
    - Type-Choose **1+1** Optimized from the drop-down list.
    - Protect Port-Choose the protect port from the drop-down list. The list displays the available OC3-4, OC3-8, or MRC-2.5G-4 ports. If OC3-4, OC3-8, or MRC-2.5G-4 cards are not installed, no ports appear in the drop-down list.
      After you choose the protect card, a list of cards available for protection appear in the Available Ports list. If no cards are available, no cards appear. If this occurs, you cannot complete this task until you install the physical cards or preprovision the ONS 15454 slots using the "DLP-A330 Preprovision a Card Slot" task.
6. From the Available Ports list, choose the port that will be protected by the port you selected in the Protect Port field. Click the top arrow button to move each port to the Working Ports list.
7. Complete the remaining fields:
    - Reversion time-If Revertive is checked, choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the primary channel is automatically renamed as secondary and the secondary channel is renamed as primary. The reversion timer starts after conditions causing the switch are cleared.
    - Verification guard time-Choose the verification guard time from the drop-down list. The range is 500ms to 1s. A verification guard timer is used to ensure the acceptance of a Force switch command from the far-end node. When the Force command is received, if no Lockout is present or if Secondary section is not in a failed state, then the outgoing K1 byte is changed to indicate Force and the verification guard timer is started. If a Force switch command is not acknowledged by the far-end within the verification guard timer duration, then the Force command is cleared.
    - Recovery guard time-Choose the recovery guard time from the drop-down list. The range is

0s to 10s. The default is 1s. A recovery guard timer is used for preventing rapid switches due to SD/SF (Signal Degrade/Signal Failure) failures. After the SD/SF failure is cleared on the line, a recovery guard timer is started. Recovery guard time is the amount of time elapsed before the system declares that a condition is cleared after the detection of an SD/SF failure.

- Detection guard time-Choose the detection guard time from the drop-down list. The range is 0s to 5s. The default is 1s. The detection guard timer is started after detecting an SD/SF/LOS (Loss of Signal) /LOF (Loss of Frame) /AIS-L (Alarm Indication Signal - Line) failure. Detection guard time is the amount of time elapsed before a traffic switch is initiated to a standby card after the detection of an SD/SF/LOS/LOF/AIS-L failure on the active card.

8. Click **OK**.
9. Return to your originating procedure (NTP).

DLP-A561 Modify an Optimized 1+1 Protection Group

Purpose	This task modifies an optimized 1+1 protection group for OC3-4, OC3-8, and MRC-2.5G-4 cards (in OC-3 configurations).
Tools/Equipment	None
Prerequisite Procedures	DLP-A560 Create an Optimized 1+1 Protection Group DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > Protection** tabs.
2. In the Protection Groups area, click the optimized 1+1 protection group you want to modify.
3. In the Selected Group area, modify the following as needed:
   - Name-Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
   - Reversion time-If Revertive is checked, choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the primary channel is automatically renamed as secondary and the secondary channel is renamed as primary.
   - Verification guard time-Choose the verification guard time from the drop-down list. The range is 500ms to 1s. A verification guard timer is used to ensure the acceptance of a Force switch command from the far-end node. When the Force command is received, if no Lockout is present or if the Secondary section is not in a failed state, then the outgoing K1 byte is changed to indicate Force and the verification guard timer is started. If a Force user command is not acknowledged by the far-end within the verification guard timer duration, then the Force command is cleared.
   - Recovery guard time-Choose the recovery guard time from the drop-down list. The range is 0s to 10s. The default is 1s. A recovery guard timer is used for preventing rapid switches due to signal degrade (SD) or signal failure (SF) failures. After the SD/SF failure is cleared on the line, a recovery guard timer is started. Recovery guard time is the amount of time elapsed before the system declares that a condition is cleared after the detection of an SD/SF failure.
   - Detection guard time-Choose the detection guard time from the drop-down list. The range is 0s to 5s. The default is 1 second. The detection guard timer is started after detecting an SD, SF, loss of signal (LOS), loss of frame (LOF), or line alarm indication signal (AIS-L) failure. Detection guard time is the amount of time elapsed before a traffic switch is initiated to a standby card after the detection of an SD, SF, LOS, LOF, or AIS-L failure on the active card.
4. Click **Apply**. Confirm that the changes appear; if not, repeat the task.

5. Return to your originating procedure (NTP).

DLP-A562 View ML-Series RPR Span PM Parameters

Purpose	This task enables you to view RPR span PM counts at selected time intervals on an ML-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note: For ML-Series card provisioning, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

1. In node view, double-click the ML-Series Ethernet card where you want to view PM counts. The card view appears.
2. Click the **Performance > RPR Span** tabs.
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 Port RPR East and Port RPR West columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

   Note: To refresh, reset, or clear PM counts, see the NTP-A253 Change the PM Display.
5. Return to your originating procedure (NTP).

DLP-A563 Configure an Automatically Routed BLSR DRI

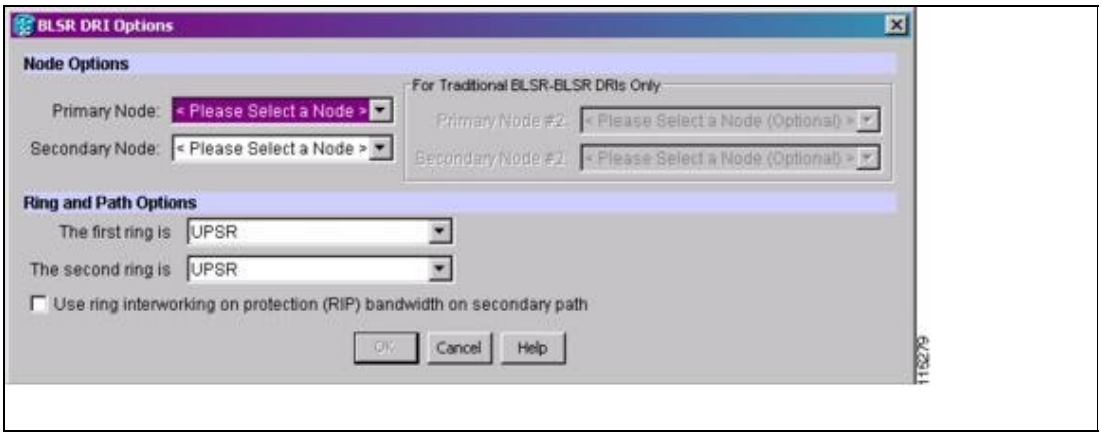
Purpose	This task enables you to set the primary and secondary nodes and ring and path options for an automatically routed BLSR Dual Ring Interconnect (DRI), as well as set circuit routing constraints.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC You must check Dual Ring Interconnect on the Circuit Creation wizard during a circuit creation procedure (automatically routed).
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In the Circuit Constraints for Automatic Routing area, click **Add BLSR DRI**.
2. In the confirmation window, click **OK**.
3. In the Node options area of the BLSR DRI Options dialog box, complete the following (Figure 22-12):
   - Primary Node-For a traditional or integrated BLSR-DRI, choose the node where the circuit interconnects the rings.
   - Secondary Node-For a traditional or integrated BLSR-DRI, choose the secondary node for the circuit to interconnect the rings. This route is used if the route on the primary node fails.
   - Primary Node #2-For a traditional BLSR-DRI where two primary nodes are required to interconnect rings, choose the second primary node.

- Secondary Node #2-For a traditional BLSR-DRI where two secondary nodes are required, choose the second secondary node.

4. In the Ring and Path Options area, complete the following:
   - The first ring is-Choose Path Protection or BLSR from the drop-down list.
   - The second ring is-Choose Path Protection or BLSR from the drop-down list.
   - Use ring interworking protection (RIP) on secondary path-Check this box to carry the secondary spans on the protection channels. These spans will be preempted during a ring/span switch.

Figure 22-12: Selecting BLSR DRI Primary and Secondary Node Assignments



5. Click **OK**. The node information appears in the Required Nodes/Lines list, and the map graphic indicates which nodes are primary and secondary.
6. In the Circuit Constraints for Automatic Routing area, click a node or span on the circuit map:
7. Click **Include** to include the node or span in the circuit, or click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit will be routed. Click spans twice to change the circuit direction. If you are creating a path protection to BLSR traditional handoff, exclude the unprotected links from the primary node towards the secondary node. If you are creating a path protection to BLSR integrated handoff, exclude unnecessary DRIs on the path protection segments.
8. Review the circuit constraints. To change the circuit routing order, choose a node in the Required Nodes/Links list and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.
9. Return to your originating procedure (NTP).

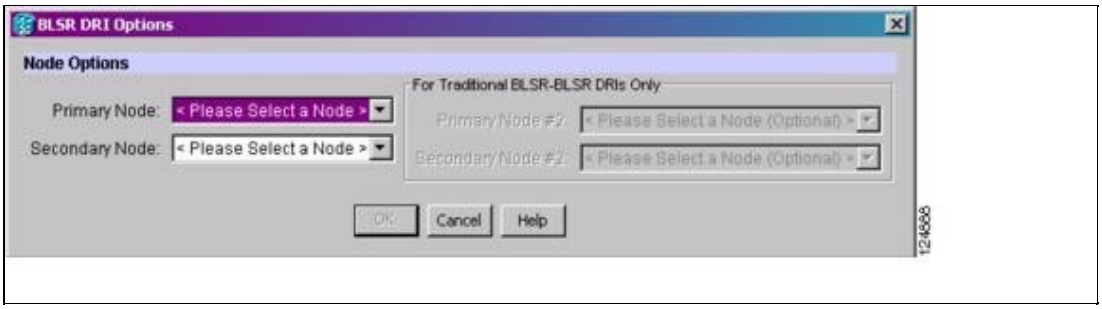
DLP-A564 Configure a Manually Routed BLSR DRI

Purpose	This task enables you to set the primary and secondary nodes for a manually routed BLSR DRI, as well as set circuit routing constraints.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC You must check Dual Ring Interconnect on the Circuit Creation wizard during a circuit creation procedure (manually routed).
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In the Route/Review Edit area, click the **BLSR-DRI Nodes** tab.

2. Click **Add BLSR DRI**.
3. In the BLSR DRI Options dialog box, complete the following (Figure 22-13):
   - Primary Node-For a traditional or integrated BLSR-DRI, choose the node where the circuit interconnects the rings.
   - Secondary Node-For a traditional or integrated BLSR-DRI, choose the secondary node for the circuit to interconnect the rings. This route is used if the route on the primary node fails.
   - Primary Node #2-For a traditional BLSR-DRI where two primary nodes are required to interconnect rings, choose the second primary node.
   - Secondary Node #2-For a traditional BLSR-DRI where two secondary nodes are required, choose the second secondary node.
4. Click **OK**.
5. Review the circuit constraints. To change the circuit routing order, choose a node in the Required Nodes/Links list and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.
6. Click the **Included Spans** tab.

Figure 22-13: Selecting BLSR DRI Primary and Secondary Node Assignments (Manual Routing)



7. Return to your originating procedure (NTP).

DLP-A565 Set Up a Solaris Workstation for a Craft Connection to an ONS 15454

Purpose	This task sets up a Solaris workstation for a craft connection to the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

1. Log into the workstation as the root user.
2. Check to see if the interface is plumbed by typing:

   #ifconfig *device*
   For example:
   #ifconfig hme1
   If the interface is plumbed, a message similar to the following appears:
   `hme1:flags=1000842BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 2 inet 0.0.0.0 netmask 0`
   If a message similar to this one appears, go to Step 4.
   If the interface is not plumbed, a message similar to the following appears:
   `ifconfig: status: SIOCGLIFFLAGS: hme1: no such interface.`

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

3. Plumb the interface by typing:

   # ifconfig *device* **plumb**
   For example:
   # ifconfig hme1 plumb
4. Configure the IP address on the interface by typing:

   # ifconfig *interface ip-address* **netmask** *netmask* **up**
   For example:
   #ifconfig hme0 192.1.0.3 netmask 255.255.255.0 up
   Note: Enter an IP address that is identical to the ONS 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254.
5. In the Subnet Mask field, type **255.255.255.0**. Skip this step if you checked Enable Socks Proxy on Port and External Network Element (ENE) at Provisioning > Network > General > Gateway Settings.
6. Test the connection:
   1. Start Netscape Navigator.
   2. Enter the ONS 15454 IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box appear. If this occurs, go to Step 2 of the "DLP-A60 Log into CTC" task to complete the login. If the Login dialog box does not appear, complete Substep 3 and 4.
   3. At the prompt, type:

      ping *ONS-15454-IP-address*
      For example, to connect to an ONS 15454 with a default IP address of 192.1.0.2, type:
      ping 192.1.0.2
      If your workstation is connected to the ONS 15454, the following message appears:
      `IP-address is alive`
      Note: Skip this step if you checked Enable Socks Proxy on Port and External Network Element (ENE) at Provisioning > Network > General > Gateway Settings.
   4. If CTC is not responding, a "Request timed out" (Windows) or a "no answer from *x.x.x.x*" (UNIX) message appears. Verify the IP and subnet mask information. Check that the cables connecting the workstation to the ONS 15454 are securely attached. Check the link status by typing:

      # ndd -set /dev/*device* instance 0
      # ndd -get /dev/*device* link_status
      For example:
      # ndd -set /dev/hme instance 0
      # ndd -get /dev/hme link_status
      A result of "1" means the link is up. A result of "0" means the link is down.
      Note: Check the man page for ndd. For example, type: #**`man ndd`**.
7. Return to your originating procedure (NTP).

DLP-A566 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-A260 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-A567 Install the CTC Launcher Application from a Release 8.5 Node

Purpose	This task installs the CTC Launcher from an ONS 15454 node running Software R8.5.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 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-A568 Connect to ONS Nodes Using the CTC Launcher

Purpose	This task connects the CTC Launcher to ONS nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

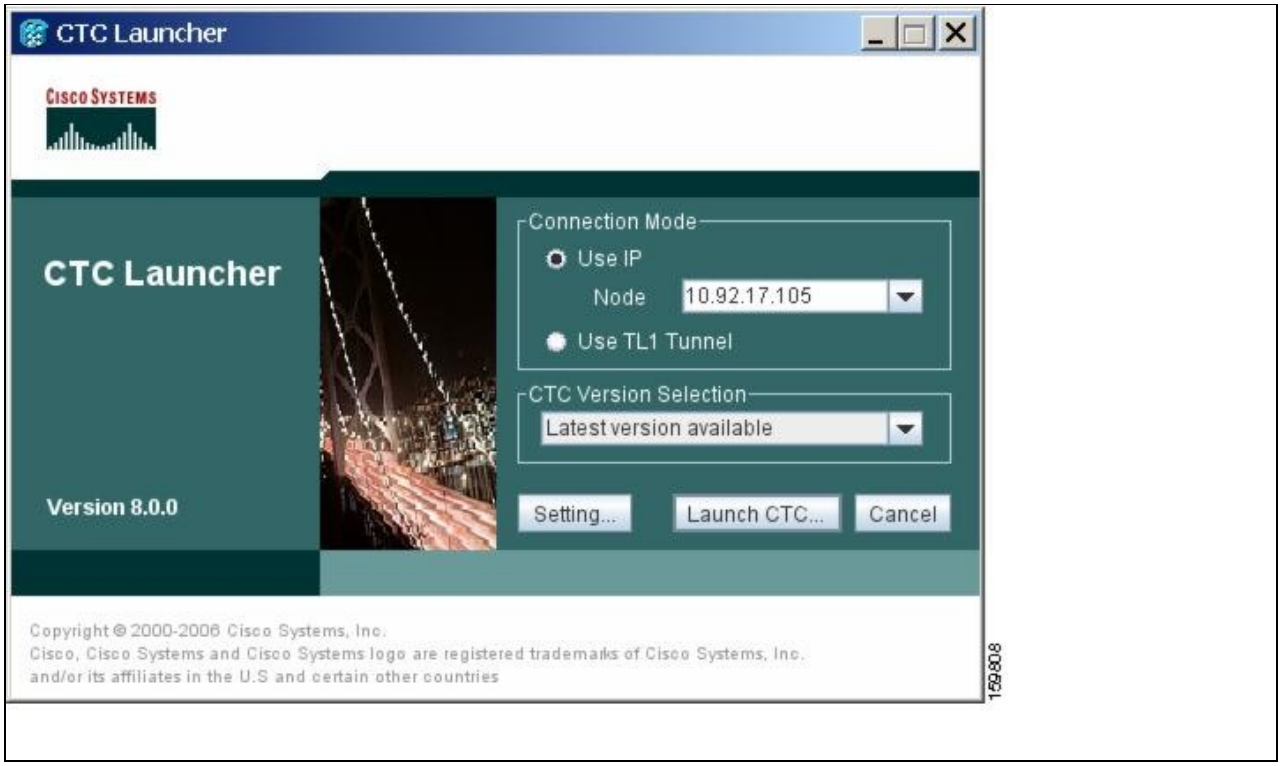
1. Start the CTC Launcher:

   - 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 shell path, navigate to the directory containing the StartCTC.exe file and type:
     % java -jar StartCTC.exe

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

Figure 22-14 shows the CTC Launcher window.

Figure 22-14: 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 needed (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).

DLP-A569 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-A260 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 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-A570 Create a TL1 Tunnel Using CTC

Purpose	This task creates a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC

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

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-A571 View TL1 Tunnel Information

Purpose	This task views a TL1 tunnel created using the CTC Launcher.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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 22-8.

Table 22-8: 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-A572 Edit a TL1 Tunnel Using CTC

Purpose	This task edits a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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-A573 Delete a TL1 Tunnel Using CTC

Purpose	This task deletes a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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-A574 Provision a PPM on the MRC-12 or MRC-2.5G-4 Card

Purpose	This task provisions single-rate and multirate pluggable port modules (PPMs) for the MRC-12 or MRC-2.5G-4 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 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 MRC-12 or MRC-2.5G-4 card where you want to provision PPM settings.
2. Click the **Provisioning > Pluggable Port Modules** tabs.
3. In the Pluggable Port Modules pane, click Create. The Create PPM dialog box appears.
4. In the Create PPM dialog box, complete the following:
   - PPM-Choose the slot number where the SFP is installed from the drop-down list.
   - PPM Type-Choose the number of ports located on the SFP from the drop-down list. If only one port is supported, PPM (1 port) is the only option.
5. Click **OK**. The newly created port appears on the Pluggable Port Modules pane. The row on the Pluggable Port Modules pane turns light blue and the Actual Equipment Type column lists the equipment name.
6. Verify that the PPM appears in the list on the Pluggable Port Modules pane. If it does not, repeat Steps 4 through 5.
7. Repeat the task to provision a second PPM.
8. Click **OK**.
9. Continue with the "DLP-A575 Provision the Optical Line Rate on the MRC-12 or MRC-2.5G-4 Card" task to provision the line rate.
10. Return to your originating procedure (NTP).

DLP-A575 Provision the Optical Line Rate on the MRC-12 or MRC-2.5G-4 Card

Purpose	This task provisions the optical line rate on a MRC-12 or MRC-2.5G-4 PPM. Regardless of whether a PPM on the MRC-12or MRC-2.5G-4 card is single-rate or multirate, you must provision the line rate on the PPM.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 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 MRC-12 or MRC-2.5G-4 card where you want to provision PPM settings.
2. Click the **Provisioning > Pluggable Port Modules** tabs.
3. In the Pluggable Ports pane, click Create. The Create Port dialog box appears.
4. In the Create Port dialog box, complete the following:

- Port-Click the PPM number and port number from the drop-down list. The first number indicates the PPM and the second number indicates the port number on the PPM. For example, the first PPM displays as 1-1 and the second PPM displays as 2-1.
- Port Type-Click the type of port from the drop-down list. The port type list displays the supported port rates on your PPM, which may differ based on PPM type and rate. See Table 22-9 for definitions of the supported rates on the MRC-12 and MRC-2.5G-4 cards.

Table 22-9: PPM Port Types

Card	Port Type
MRC-12 and MRC-2.5G-4	• OC-3-155 Mbps • OC-12-622 Mbps • OC-48-2.48 Gbps

5. Click **OK**.
6. Repeat Steps 3 through 5 to configure the port rates as needed.
7. Click **OK**. The row on the Pluggable Ports pane is light blue until the actual SFP is installed and then the row turns white.
8. Return to your originating procedure (NTP).

DLP-A576 Change the Optical Line Rate on the MRC-12 or MRC-2.5G-4 Card

Purpose	This task changes the optical line rate on a multirate PPM. Perform this task if you want to change the port rate on an SFP that is already provisioned.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 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 MRC-12 or MRC-2.5G-4 card where you want to provision PPM settings.
2. Click the **Provisioning > Pluggable Port Modules** tabs.
3. Click the port with the port rate you want to change in the Pluggable Ports pane. The highlight changes to dark blue.
4. Click Edit. The Edit Port Rate dialog box appears.
5. In the Change To field, use the drop-down list to select the new port rate and click **OK**.
6. Click **Yes** in the Confirm Port Rate Change dialog box.
7. Return to your originating procedure (NTP).

DLP-A577 Delete a PPM from the MRC-12, MRC-2.5G-4, or OC192-XFP Card

Purpose	This task deletes PPM provisioning for SFPs on the MRC-12, MRC-2.5G-4, or OC192-XFP card.
Tools/Equipment	None

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

1. Determine if the PPM can be deleted.

   You cannot delete a port on a PPM if it is in service, part of a protection group, has a communications channel termination in use, is used as a timing source, has circuits, or has overhead circuits. As needed, complete the following procedures and task:

   - DLP-A154 Modify a 1+1 Protection Group
   - NTP-A85 Change Node Timing
   - NTP-A292 Modify or Delete Communications Channel Terminations and Provisionable Patchcords
   - NTP-A151 Modify and Delete Circuits
   - NTP-A278 Modify and Delete Overhead Circuits and Server Trails
   - DLP-A214 Change the Service State for a Port

2. In node view, double-click the card where you want to delete PPM settings.
3. Click the **Provisioning > Pluggable Port Modules** tabs.
4. To delete a PPM and the associated ports:
   1. Click the PPM line that appears in the Pluggable Port Modules pane. The highlight changes to dark blue.
   2. Click Delete. The Delete PPM dialog box appears.
   3. Click **Yes**. The PPM provisioning is removed from the Pluggable Port Modules pane and the Pluggable Ports pane.
5. Verify that the PPM provisioning is deleted:

   · If the PPM was preprovisioned, CTC shows an empty slot in CTC after it is deleted.
   · If the SFP (PPM) is physically present when you delete the PPM provisioning, CTC transitions to the deleted state; the ports (if any) are deleted, and the PPM is represented as a gray graphic in CTC. The SFP can be provisioned again in CTC or the equipment can be removed, in which case the removal causes the graphic to disappear.
6. If you need to remove the SFP, see the "DLP-A470 Remove GBIC or SFP/XFP Devices" task.
7. Return to your originating procedure (NTP).

DLP-A578 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-A567 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,

◊ Click **Tools > Internet Options**.

2. Click **Security** tab.
3. Select the zone that is appropriate. Available options are: Local Intranet ,Internet, and Trusted Sites.
4. 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-A579 Provision an Open VCAT Circuit Source and Destination

Purpose	This task provisions an open virtual concatenated (VCAT) circuit source and destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC The Circuit Creation wizard Circuit Source page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. From the Node drop-down list, choose the node where the circuit will originate.
2. From the Slot drop-down list, choose the slot containing the CE-Series, ML-Series, or FC_MR-4 card where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the list.)
3. Depending on the circuit origination card, choose the source port and/or STS and, if applicable, VT from the Port and STS drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs and VTs do not appear if they are already in use by other circuits. VTs do not appear for STS-V circuits.
4. Click **Next**.
5. Click the Auto-ranged Destinations check box to select the endpoints automatically. Only the first endpoint has to be selected, all of the other endpoints will be automatically created.

If you do not choose auto-ranged destinations; from the card selected in Step 2, choose the source port and/or STS and, if applicable, VT from the Port and STS drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs and VTs do not appear if they are already in use by other circuits. VTs do not appear for STS-V circuits.

6. From the Select Destinations For drop-down list, choose the member number.
7. From the Node drop-down list, choose the destination node.
8. From the Slot drop-down list, choose the slot containing the card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.) Non-data cards may be used for open VCAT circuits.
9. Click **Add Destinations**.
10. Click **Next**.
11. Return to your originating procedure (NTP).

DLP-A580 Create User Defined Alarm Types

Purpose	This task creates alarm types for external alarms on the AIC-I card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 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 AIC-I card.
2. Click the **Provisioning > User Defined Alarms** tabs.
3. Click Add.The Enter New Alarm Type dialog box appears.
4. In the name field type the new alarm type name and click **OK**.
   - The name can be up to 20 alphanumeric characters (upper case). No spaces, no special characters, hyphen (-) is allowed.
   - Up to 50 different Alarm Types can be defined.
5. Click the **External Alarms** tab.
6. Verify that the defined name appears in the Alarm Type drop-down list.
7. Return to your originating procedure (NTP).

DLP-A 581 Configure Link Integrity Timer

Purpose	This task sets the link integrity soak timer for each port in the Ethernet cards (mapper cards).
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 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 OOS,DSBLD or OOS,MT 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-A595 Provision Card Mode for CE-MR-10 Card

Purpose	This task provisions the card mode for the CE-MR-10 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: When you change the provisioning mode, the card should not have any circuits configured on it.

1. In the node view, double-click the CE-MR-10 card.
2. Click the **Provisioning > Card** tabs.
3. In the Mode drop-down list, select one of the following:
   - MANUAL-Allows the selection of STS during circuit creation.
   - AUTOMATIC-Prevents the selection of STS during circuit creation.
4. Click **Apply**.
5. Return to your originating procedure (NTP).