Maintaining the Node

This chapter provides procedures for maintaining the nodes, including database backup and restoration, removing and replacing cards, viewing the audit trail, and hardware maintenance procedures such as cleaning fibers, changing the fan tray filter, and other maintenance procedures.

Note The procedures and tasks described in this chapter for the Cisco ONS 15454 platform is applicable to the Cisco ONS 15454 M2 and Cisco ONS 15454 M6 platforms, unless noted otherwise.

Note Unless otherwise specified, "ONS 15454" refers to both ANSI and ETSI shelf assemblies.

Chapter procedures include:

Optical SMU

Optical SMU Considerations

- Only one SMU can be active at a time.
- SMUs are supported on the TCC3, TNC, TSC, TNC-E, and TSC-E cards. SMUs are not supported in TCC2P card, Cisco ONS 15454 DWDM lite and MSPP packages. SMUs are supported from release 10.3.
- SMUs are cumulative. The latest SMU includes all the previous SMUs.

  For example, bugs 1, 2, and 3 are addressed in SMU A; bugs 1, 2, 3, 4, and 5 in SMU B; bugs 1, 2, 3, 4, 5, 6, 7, and 8 in SMU C. In this case, the user can download and activate the latest SMU (SMU C) on the relevant nodes.
- SMUs are release specific. The same bug fix in two releases is packaged in two separate SMUs.
- SMUs are persistent. SMUs are re-applied when the card is soft or hard reset.
- SMUs are not supported in FPGA changes, CTC files, and DM agents.

NTP-G347 Managing SMUs Using CTC

Purpose	This procedure allows you to manage SMUs using CTC .
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following tasks as needed:

- DLP-G779 Downloading, Activating, and Disabling an SMU on the Node Using CTC, on page 3
- DLP-G780 Downloading and Activating an SMU on Multiple Nodes Using CTC, on page 3

Stop. You have completed this procedure.

DLP-G779 Downloading, Activating, and Disabling an SMU on the Node Using CTC

Purpose	This task allows you to download, activate, disable an SMU on the node using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Maintenance** > **Software** > **Software Patch Management** tabs.

The node name, downloaded SMU, active SMU and the time Stamp (indicating the time of last activity on the SMU) are displayed. When there is no SMU on the node, only the node name is displayed. The Active and Downloaded columns are empty.

Step 2 Click **Download**.

Step 3 Browse and select the appropriate SMU file. The SMU file ends with .smu extension.

Step 4 In the Download Selection dialog, check the appropriate check box to select the node on which you wish to download the SMU.

Step 5 Click **OK**.

The SMU file is downloaded and listed (but not activated) in the Downloaded column.

Step 6 To activate the SMU, select the row and click **Activate**.

The downloaded SMU is now active and is listed in the Active column. If the downloaded file is already active on the node, this activation step is not allowed.

Step 7 To disable and delete the SMU, select the row and click **Disable**.

A warning message is displayed that disabling the patch might cause traffic loss.

Step 8 Click **Yes** to disable and delete the patch.

Step 9 Return to your originating procedure (NTP).

DLP-G780 Downloading and Activating an SMU on Multiple Nodes Using CTC

Purpose	This task allows you to download and activate an SMU on multiple nodes using CTC.

Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In network view, click the **Maintenance** > **Software** > **Software Patch Management** tabs.

Step 2 Click **Get Patch Info**.

The nodes running Release 10.3 and above are displayed in this dialog.

Step 3 Select the nodes on which you wish to download the SMU and click **OK**.

The selected nodes are displayed in the Software Patch Management pane.

Step 4 Click **Download** to download the SMU on all the selected nodes.

Step 5 Click **Activate** to activate the SMU on all the selected nodes.

Step 6 Return to your originating procedure (NTP).

Cooling Profile

The cooling profile feature allows you to control the speed of the fans in the ONS 15454 M6 shelf depending on the I/O cards used.

The user can enable automatic cooling profile or manual cooling profile at the node level. The automatic cooling profile is selected by default from R10.3. In this case, the cooling profile of the shelf is set based on the line cards used in the shelf. The supported cooling profile values are Low, Medium, and High. The default cooling profile value is High.

You can change the cooling profile of the node from automatic to manual. In this case, the user needs to change the cooling profile of the shelf depending on the line cards used in the shelf. If there are multiple cards in the shelf, you must choose the cooling profile of the card that requires the highest cooling profile. For example, if the shelf has two cards with low cooling profile, three cards with medium cooling profile, and one card with high cooling profile, you must choose a high cooling profile for the shelf.

⚠ **Caution** The wrong cooling profile chosen for the shelf might harm the cards present in the shelf.

When the database is restored after the backup, there might be a mismatch in cooling profile at the node level. Hence, it is recommended to set the cooling profile of the node to manual and then set to automatic to recalculate the cooling profile based on the line cards.

When an incorrect cooling profile is chosen for the shelf, the Cool Mismatch (COOL-MISM) alarm is raised on the shelf. For more information on the alarm, see the "COOL-MISM" alarm in Chapter 2, Alarm Troubleshooting of *Cisco ONS 15454 DWDM Troubleshooting Guide*.

NTP-G354 Enabling Cooling Profile Using CTC

Purpose	This task allows you to enable automatic or manual cooling profile for the node and shelves using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Enable automatic cooling profile for the node and shelves.

a) In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **General** tabs.

b) Uncheck the **Enable Manual Cooling** check box.

c) In shelf view, click the **Provisioning** > **General** > **Voltage/Temperature** tabs.

The cooling profile of each shelf is set in the Cooling Profile drop-down list depending on the line cards used in the shelf.

Step 2 Enable manual cooling profile for the node and shelves.

a) In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **General** tabs.

b) Check the **Enable Manual Cooling** check box.

c) In shelf view, click the **Provisioning** > **General** > **Voltage/Temperature** tabs.

d) From the Cooling Profile drop-down list, choose the appropriate cooling profile value of the shelf depending on the line cards used in the shelf.

The supported cooling profile values are Low, Medium, and High. The default cooling profile value is High.

Stop. You have completed this procedure.

Power Redundancy

You can configure the power redundancy mode of an NCS 2015 chassis using CTC or TL1 commands. You can also unselect the power modules that are not used and avoid alarms for those power modules.

When you plug in a DC power module, by default, the type is configured as None (neither Work nor Protect). You must manually configure the power module as Work or Protect. The power calculation and alarms related to this module are analyzed and raised only when the power module is configured as Work, Protect, or Work and Protect. For more information, see NTP-G358 Configuring a Power Redundancy Mode, on page 8

Note This feature is supported only on Cisco NCS 2015.

Table 1: Feed Settings of Cisco NCS 2015 DC Power Module

Type of Power Module	Feed A	Feed B
Work	Mandatory	Optional
Protect	Optional	Mandatory
Work and Protect	Mandatory	Mandatory

Note There are no mandatory settings related to any physical feed for a Cisco NCS 2015 AC power module.

Power Redundancy Mode

Note For any power redundancy mode, the Work (W), Protect (P), and Work Protect (WP) combinations must match the table below. However, the participating power modules can be any of the Power 1, Power 2, Power 3, or, Power 4 modules.

Table 2: Supported Power Redundancy Modes for DC and AC Power, Maximum Power, and Alarm Severity

Power Redundancy Mode	Supported for DC Power	Supported for AC Power	Power 1	Power 2	Power 3	Power 4	Maximum Power for DC	Maximum Power for AC	Alarm Severity
1+0	Yes	Yes	W	—	—	—	1750	3000	Any failure of the power module is of default severity.

Power Redundancy Mode	Supported for DC Power	Supported for AC Power	Power 1	Power 2	Power 3	Power 4	Maximum Power for DC	Maximum Power for AC	Alarm Severity
1+1	Yes	Yes	W	P	—	—	1750	3000	First failure of the power module is minor, further failure is of default severity on the power module of the lower index.
2+0	Yes	Yes	W	W	—	—	3500	6000	Any failure of the power module is of default severity.
2+1	Yes	No	W	P	WP	—	3500	—	First failure of the power module is minor, further failure is of default severity on the power module of the lower index.
3+0	Yes	No	W	W	W	—	5250	—	Any failure of the power module is of default severity.
3+1	Yes	No	W	P	WP	WP	5250	—	First failure of the power module is minor, further failure is of default severity on the power module of the lower index.
2+2	Yes	Yes	W	W	P	P	3500	6000	First two failures of the power modules are minor, further failure is of default severity on the power module of the lower index.

Power Alarms

The Feed Mismatch alarm is a new alarm introduced in Release 10.5.1. This alarm is raised when the mandatory input feed of the DC power module is not connected or is incorrectly connected. The polling interval for this alarm is 15 mins and the alarm gets raised or cleared within this interval. The polling also occurs for a particular Power Supply Unit (PSU) when there is configuration change or when it is plugged out or plugged in. For an AC power module of a Cisco NCS 2015, the feed mismatch alarm is raised when the power module is not connected to an appropriate power source.

The following are the power alarms:

- EQPT-MISS

- BAT-FAIL
- FEED-MISMATCH
- MFGMEM

For more information on the above alarms, see the *Cisco NCS 2000 Series Troubleshooting Guide, Release 10.x.x*.

Power Redundancy Mode While Upgrading from Release 10.5

When you upgrade from Release 10.5, or perform a fresh install of Release 10.5.2, the default power redundancy mode depends on the number of power modules plugged into the Cisco NCS 2015. For more information on configuring the power redundancy mode using CTC, see NTP-G358 Configuring a Power Redundancy Mode, on page 8.

Table 3: Default Power Redundancy Mode on Upgrade or Fresh Install

Number of Power Modules Detected	Redundancy Mode Configured for DC Power	Redundancy Mode Configured for AC Power
1	1+0	1+0
2	2+0	2+0
3	3+0	2+0
4	3+0	2+0

The default power redundancy mode configuration is according to the table above. If you want to configure a mode different from the default mode, you must manually configure the mode using CTC or TL1 commands.

NTP-G358 Configuring a Power Redundancy Mode

Purpose	(Cisco NCS 2015) This task lets you configure the power redundancy of an NCS 2015 chassis.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Procedure

Step 1 In the shelf view, click the **Provisioning** > **General** > **Power Monitor** tabs.

Step 2 In the **Power Supply Unit (PSU) Configuration** area, check the **Work** and **Protect** check boxes for any PSU according to the power redundancy mode that you want to configure.

Note

- SNMP support is not available for PSU configuration.

Note The PWR-CON-LMT alarm is raised in the Alarms tab in CTC when the installation or pre-provisioning of a card causes the power consumption to exceed the power limit of the configured power redundancy mode. The alarm clears when the power redundancy mode is set to a higher configuration.

When you revert to the previous power redundancy mode configuration, the PWR-CON-LMT alarm is raised again and the total power consumption value in the Chassis Power Summary area displays a different value.

Step 3 Click **Apply**.

Stop. You have completed this procedure.

Examples for Configuring a Power Redundancy Mode

1. To configure a 2+0 power redundancy mode, you must select any two PSUs as Work.
2. To configure a 2+1 power redundancy mode, you must select one PSU as Work, one PSU as Protect, and another PSU as Work and Protect. For example, you can check the following check boxes:
   - PSU 1 as Work
   - PSU 2 as Protect
   - PSU 3 as Work and Protect
3. To configure a 2+2 power redundancy mode, you must select any two PSUs as Work and the other two PSUs as Protect. For example, you can check the following check boxes:
   - PSU 1 as Work
   - PSU 2 as Protect
   - PSU 3 as Work
   - PSU 4 as Protect
4. To configure a 3+1 power redundancy mode, you must select any two PSUs as Work and Protect, one PSU as Work, and another PSU as Protect. For example, you can check the following check boxes:
   - PSU 1 as Work
   - PSU 2 as Protect
   - PSU 3 as Work and Protect
   - PSU 4 as Work and Protect

Node Recovery

Database loss can happen with the provisioning database as well as the system database. In Release 10.6.2, two enhancements have been introduced to recover the node with no traffic loss. The two enhancements are described below.

- **Provisioning Database**

  When provisioning database loss occurs, a BAD-DB-DETECTED critical alarm is raised at the node level. This occurs during reboot of control cards, switchovers, or upgrades. During this time, traffic on the shelf is not affected. The line cards are in loading or software download state. The LED status on the line cards is off. The communication between the control cards and line cards is blocked to prevent provisioning. To clear the BAD-DB-DETECTED alarm, restore a previously saved database or use the "Reset NE to Factory Defaults" option to restore the node to factory default configuration. Resetting the NE to factory defaults is traffic impacting.

  Provisioning database loss also occurs during system mode conversions, reset to factory defaults or in new installations. During this time, traffic on the shelf is not affected. The line cards are in loading or software download state. The LED status on the line cards is off. A NODE-FACTORY-MODE critical alarm is raised at the node level. To clear this alarm, use the Rebuild DB option in the Maintenance > Database tabs in CTC. This procedure is traffic impacting.

  Limitations:

  When the BAD-DB-DETECTED or NODE-FACTORY-MODE alarm is raised on the near-end node , the following behavior is noticed on the near-end and far-end nodes:

  - Alarms raised on line cards are not reported.
  - GCC, DCC, and OSC links are down at the far-end node.
  - The shelf timing goes to Holdover mode on the near-end node.
  - The NODE-FACTORY-MODE and BAD-DB-DETECTED alarms do not persist after active control card resets such as soft resets, hard resets, WatchDogTimer (WDT) expiry, and node(NC/SA) power cycle. The node recovers when the current database is applied on the node. Traffic is impacted after the active control card is reset.
  - The NODE-FACTORY-MODE and BAD-DB-DETECTED alarms are not reported on the SNMP interface. These alarms are reported only on the TL1 and CTC interfaces.
  - SIGLOSS or LOS alarms are raised on the TNC OSC ports at the far-end node.
  - All the alarms that were present before the BAD-DB-DETECTED or NODE-FACTORY-MODE alarms were raised are lost and no longer reported in the Alarms tab in CTC. They can be found in the node history pane.

  When the BAD-DB-DETECTED alarm is raised on the node:

  - Existing alarms on the power modules are lost . New alarms on the power modules are not reported for Cisco NCS 2015 shelf.
  - Existing BAT-FAIL and EQPT-MISS alarms on the Cisco ONS 15454 M6 shelf are not lost.

- **System Database**

When system database loss occurs on the active or standby control card, an INVALID SYSDB alarm is raised on the control card. To clear the alarm do any of the following actions:

- If the alarm is raised only on the active control card, reboot the active card.
- If the alarm is raised only on the standby control card, reboot the standby card.
- If the alarm is raised on both the active and standby control cards, contact TAC for support.

NTP-G103 Backing Up the Database

Purpose	This procedure stores a backup version of the controller card software database on the workstation running Cisco Transport Controller (CTC) or on a network server.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	Required. Cisco recommends performing a database backup at approximately weekly intervals and prior to and after configuration changes.
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

The database write cycle is 30 seconds. After provisioning change is performed on the node, it is recommended that a user wait for at least 30 seconds before backing up the database.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Maintenance** > **Database** tabs.

Step 2 Click **Backup**.

Step 3 Save the database on the workstation’s hard drive or on network storage. Use an appropriate file name with the DB file extension; for example, database.db.

Step 4 Click **Save**.

Step 5 Click **OK** in the confirmation dialog box.

Stop. You have completed this procedure.

NTP-G104 Restoring the Database

Purpose	This procedure restores the controller card software database, either partially or completely.

Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC • NTP-G103 Backing Up the Database
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note You must back up and restore the database for each node on a circuit path in order to maintain a complete circuit.

Note During the database restore process, GMPLS circuits provisioned after the database was backed up may go into the partial state. When this occurs, delete and recreate the GMPLS circuits to revert to the discovered state.

Caution If you are restoring the database on multiple nodes, wait approximately one minute after the controller card reboot has completed on each node before proceeding to the next node.

Caution TCC2P/TCC3/TNC/TNCE/TSC/TSCE/TNCS cards can be used in single IP address (repeater) and dual IP address (secure) mode. The secure mode has advanced features that affect database restore. A database from a secure node cannot be loaded on an unsecure repeater node. A repeater mode database can be loaded onto a secure node but the database will follow the node characteristics (that is, it will become secure). A secure database cannot be loaded onto a TCC2; only TCC2P/TCC3/TNC/TNCE/TSC/TSCE/TNCS cards support secure mode. For more information about the dual IP secure mode, see the NTP-G26 Setting Up CTC Network Access procedure. Also refer chapter, Managing Network Connectivity.

Note Due to memory limitations, TCC2/TCC2P cards are not supported from Release 10.5.2 onwards. As a result, in a multishelf configuration, the TCC2/TCC2P card cannot be a node controller or a shelf controller. Upgrade the TCC2/TCC2P card to a TCC3 card

Note When a database restore operation is performed on a node using the database of another node that contains a 15454-M-FILLER card, the 15454-M-FILLER card is displayed as a pre-provisioned unit in CTC on the restored node. This is not seen if that specific slot is already installed with a line card.

To delete the pre-provisioned 15454-M-FILLER card on the restored node, plug-in a 15454-M-FILLER card in that pre-provisioned slot and then plug-out the FILLER card to delete the card from CTC.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Circuits** tab. Verify that no optical channel network connection (OCHNC) circuits have a PARTIAL_OOS state. If so, investigate and resolve the partial state before continuing.

Step 2 Complete the DLP-G157 Disable Automatic Power Control task

Step 3 In multishelf view (multishelf mode) or in node view (single-shelf mode), click the **Maintenance** > **Database** tabs.

Step 4 Click **Restore**.

Step 5 Locate the database file stored on the workstation hard drive or on network storage.

Note To clear all existing provisioning, locate and upload the database found on the latest software CD.

Step 6 Click the database file to highlight it.

Step 7 Click **Open**. The DB Restore dialog box appears.

Caution Opening a restore file from another node or from an earlier backup might affect traffic on the login node.

Step 8 If you need a complete database restore, check the **Complete database (System and Provisioning)** checkbox. Continue with Step 10.

Note The following parameters are restored only when the **Complete Database (System and Provisioning)** checkbox is checked: node name, IP address, subnet mask and gateway, and IIOP port. If you change the node name and then restore a backed up database on this node, the circuits automatically map to the newly renamed node. It is recommended to keep a record of the old and new node names.

Note Complete database restore may be used only on a node that is removed from the network, and does not carry live provisioning traffic. This operation needs to be done by a live operator onsite, and must not use a remote connection.

Step 9 If you need to restore only the provisioning database (partial restore), do not check the **Complete database (System and Provisioning)** checkbox.

Step 10 Click **Ok**.

The Restore Database dialog box monitors the file transfer.

Note You cannot cancel the database restore operation.

Step 11 Wait for the file to complete the transfer to the controller card.

Step 12 Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears. Wait for the node to reconnect.

Step 13 Complete the DLP-G158 Enable Automatic Power Control task.

Stop. You have completed this procedure.

NTP-G105 Restoring the Node to Factory Configuration

Purpose	This procedure reinitializes the Cisco ONS 15454, ONS 15454 M2,and ONS 15454 M6 using the CTC reinitialization tool. Reinitialization uploads a new software package to the controller cards, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15454 System Software CD JRE 1.6 is recommended to log into the node after reinitialization is complete. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 1.6.
Prerequisite Procedures	NTP-G103 Backing Up the Database NTP-G17 Set Up Computer for CTC One of the following: • NTP-G18 Set Up CTC Computer for Local Craft Connection to the ONS 15454 • NTP-G19 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser only

⚠ **Caution** Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinitialization tool chooses the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You might accidentally copy an incorrect database if multiple databases are kept in the specified directory.

⚠ **Caution** Restoring a node to the factory configuration deletes all cross-connects on the node.

⚠ **Caution** Cisco recommends that you save the node database to safe location if you will not be restoring the node using the database provided on the software CD.

Note A node will remain locked in secure mode even if it is restored with the factory database. A node locked in secure mode can only be unlocked by Cisco Technical Support.

Procedure

Step 1 If you need to install or replace one or more TCC2/TCC2P/TCC3 cards, see the task,DLP-G33 Installing the TCC2, TCC2P, or TCC3 Card. If you need to install one or more TNC/TNCE/TSC/TSCE cards, see the task, DLP-G604 Installing the TNC, TNCE, TSC, or TSCE Card .

Note Due to memory limitations, TCC2/TCC2P cards are not supported from Release 10.5.2 onwards. As a result, in a multishelf configuration, the TCC2/TCC2P card cannot be a node controller or a shelf controller. Upgrade the TCC2/TCC2P card to a TCC3 card.

Step 2 If you are using Microsoft Windows, complete the task, DLP-G248 Using the Reinitialization Tool to Clear the Database and Upload Software.

Step 3 If you are using UNIX, complete the procedure, NTP-G273 Changing the System Mode.

Stop. You have completed this procedure.

DLP-G248 Using the Reinitialization Tool to Clear the Database and Upload Software

Purpose	This task reinitializes the Cisco ONS 15454, ONS 15454 M2, and ONS 15454 M6 using the CTC reinitialization tool on a Windows or UNIX computer. Reinitialization uploads a new software package to the controller cards, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15454 System Software CD JRE 1.6 must be installed on the computer to log into the node at the completion of the reinitialization. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 1.6.

Prerequisite Procedures	NTP-G103 Backing Up the Database NTP-G17 Set Up Computer for CTC One of the following: • NTP-G18 Set Up CTC Computer for Local Craft Connection to the ONS 15454 • NTP-G19 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454
Required/As Needed	As needed to clear the existing database from the controller cards and restore the node default settings.
Onsite/Remote	Onsite
Security Level	Superuser only

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

Note A node will remain locked in secure mode after the node's database is deleted, even if it is restored with the factory database. A node locked in secure mode can only be unlocked by Cisco Technical Support.

Procedure

Step 1 Insert the ONS 15454 system software CD , into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 To run the recovery tool file:

- Windows—From the Windows Start menu, choose **Run.** In the Run dialog box, click **Browse** and navigate to the CISCO15454 or CISCO15454SDH folder on the software CD. Choose the RE-INIT.jar file and click **Open**.
- UNIX—Navigate to the CISCO15454 directory on the CD (usually /cdrom/cdrom0/CISCO15454 or /cdrom/cdrom0/CISCO15454SDH). If you are using a file explorer, double-click the RE-INIT.jar file. If you are working with a command line, run java -jar RE-INIT.jar.

  The NE Re-Initialization window appears.

Step 3 Complete the following fields:

- GNE IP—If the node you are reinitializing is accessed through another node configured as a gateway network element (GNE), enter the GNE IP address. If you have a direct connection to the node, leave this field blank.
- Node IP—Enter the node name or IP address of the node that you are reinitializing.
- User ID—Enter the user ID needed to access the node.

- Password—Enter the password for the user ID.
- Upload Package—Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
- Force Upload—Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
- Activate/Revert—Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tab.
- Confirm—Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.
- Database restore-Check this box if you want to send a new database to the node and to restore node provision values. (This is equivalent to the CTC database restore with the "Complete Database" check box unchecked.)
- Complete database restore-Check this option to send a new database to the node and to restore node provision and system values. (This is equivalent to the CTC database restore with the "Complete Database" check box checked.)
- No database restore-Check this box if you do not want the node database to be modified.
- Search Path—Enter the path to the CISCO15454 or CISCO15454SDH folder on the CD drive.

Step 4 Click **Go**.

Caution Before continuing with the next step, verify that the database to upload is correct. You cannot reverse the upload process after you click **Yes**.

Step 5 Review the information in the Confirm NE Re-Initialization dialog box, then click **Yes** to start the reinitialization.

The reinitialization begins. After the software is downloaded and activated, and the database is uploaded to the controller cards, “Complete” appears in the status bar, and the controller cards reboot. Wait a few minutes for the reboot to complete.

Step 6 After the reboot is complete, log into the node using the DLP-G46 Log into CTC task.

Step 7 Complete the procedures, NTP-G24 Setting Up Name, Date, Time, and Contact Information and NTP-G26 Setting Up CTC Network Access .

Step 8 Return to your originating procedure (NTP).

NTP-G346 Resetting the Network Element to Factory Defaults

Purpose	This procedure removes the data in the node and resets to factory default settings. The system database is retained during the reset; hence, the IP address of the node and multi-shelf configurations are retained.

Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view of the network element, click the **Provisioning** > **General** tabs.

Step 2 Click **Reset NE to Factory Defaults** to reset the network element to factory default settings.

The node starts to reboot and all the configurations will be reset to factory defaults.

Stop. You have completed this procedure.

NTP-G273 Changing the System Mode

Purpose	This procedure changes the Cisco ONS 15454 M2 and ONS 15454 M6 system mode from ANSI (SONET) to ETSI (SDH) or vice-versa. This procedure applies to the ONS 15454 M2 chassis and ONS 15454 M6 chassis in simplex mode and standalone mode.
Tools/Equipment	PC or UNIX workstation.
Prerequisite Procedures	• DLP-U546 Download the ONS 15454 Software • DLP-U546 Download the ONS 15454 SDH Software • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 (ONS 15454 M6 only) Ensure that the ONS 15454 M6 chassis is in simplex and standalone mode contains only one controller card (active TNC, TNCE, TSC, or TSCE card).

Step 2 In the node view, click the **Provisioning** > **General** > **General** tabs. The System Mode field displays the system mode as ANSI or ETSI.

Step 3 Click **Change System Mode** to toggle the system mode between ANSI and ETSI. Changing the system mode erases all the provisioned data and the system will revert to the factory default settings.

Step 4 Click **Yes**. The node reboots after the system mode change is completed. This takes about 5 minutes.

Step 5 Exit CTC. Click **File** > **Exit** menu option to exit CTC.

Step 6 Verify that the system mode has changed:

a) Complete the DLP-G46 Log into CTC task on the ONS 15454 M2 or 15454 M6 chassis where you changed the system mode.

b) In the node view, click the **Provisioning** > **General** > **General** tabs. The System Mode field indicates if the system mode has changed.

Step 7 (ONS 15454 M6 only) Insert the standby controller card (TNC, TNCE, TSC, or TSCE card). This synchronizes the software from the active controller card to the standby controller card.

Stop. You have completed this procedure.

NTP-G133 Viewing and Managing OSI Information

Purpose	This procedure allows you to view and manage Open Systems Interconnection (OSI) including the End System to Intermediate System (ES-IS) and Intermediate System to Intermediate System (IS-IS) routing information tables, the Target Identifier Address Resolution Protocol (TARP) data cache, and the manual area table.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC • NTP-G103 Backing Up the Database • NTP-G17 Set Up Computer for CTC • NTP-G132 Provisioning OSI
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following tasks as needed:

- DLP-G298 Viewing IS-IS Routing Information Base
- DLP-G299 Viewing ES-IS Routing Information Base

- DLP-G300 Managing the TARP Data Cache

Stop. You have completed this procedure.

DLP-G298 Viewing IS-IS Routing Information Base

Purpose	This task allows you to view the 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-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Maintenance** > **OSI** > **IS-IS RIB** tabs.

Step 2 View the following RIB information for Router 1:

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

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

Step 4 Return to your originating procedure (NTP).

DLP-G299 Viewing ES-IS Routing Information Base

Purpose	This task allows you to view the ES-IS protocol RIB. ES-IS is an OSI protocol that defines how end systems (hosts) and intermediate systems (routers) learn about each other. For ESs, the ES-IS RIB shows the network view from the perspective of the ES node. For ISs, the ES-IS RIB shows the network view from the perspective of the IS node.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Maintenance** > **OSI** > **ES-IS RIB** tabs.

Step 2 View the following RIB information for Router 1:

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

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

Step 4 Return to your originating procedure (NTP).

DLP-G300 Managing 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-G46 Log into CTC
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Maintenance** > **OSI** > **TDC** tabs.

Step 2 View the following TDC information:

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

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

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

a) Click the **TID to NSAP** button.
b) In the TID to NSAP dialog box, enter the TID you want to map to an NSAP.
c) Click **OK**, then click **OK** in the information message box.
d) On the TDC tab, click **Refresh**.

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

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

Step 5 Return to your originating procedure (NTP).

NTP-G106 Resetting Cards Using CTC

Purpose	This procedure resets the controller and DWDM cards using CTC.
Tools/Equipment	None

Prerequisite Procedures	• DLP-G46 Log into CTC • DLP-G33 Installing the TCC2, TCC2P, or TCC3 Card • DLP-G604 Installing the TNC, TNCE, TSC, or TSCE Card
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 As needed, complete the task, DLP-G250 Resetting the Controller Card.

Step 2 As needed, complete the task, DLP-G251 Resetting DWDM Cards Using CTC.

Stop. You have completed this procedure.

DLP-G250 Resetting the Controller Card

Purpose	This task resets the controller card and switches the node to the redundant controller card.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G33 Installing the TCC2, TCC2P, or TCC3 Card • DLP-G604 Installing the TNC, TNCE, TSC, or TSCE Card • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Note

- Before you reset the controller card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.
- The ONS 15454 M2 chassis do not have a redundant controller card.

Note

- (On ONS 15454 shelf) When a software reset is performed on an active TCC2/TCC2P/TCC3, the AIC-I card goes through an initialization process and also resets. The AIC-I card reset is normal and happens each time an active TCC2/TCC2P/TCC3 card goes through a software-initiated reset.
- Due to memory limitations, TCC2/TCC2P cards are not supported from Release 10.5.2 onwards. As a result, in a multishelf configuration, the TCC2/TCC2P card cannot be a node controller or a shelf controller. Upgrade the TCC2/TCC2P card to a TCC3 card

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Alarms** tab.

a) Verify that the alarm filter is not on. See the DLP-G128 Disable Alarm Filtering task as necessary.

b) Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 DWDM Troubleshooting Guide* for procedures.

Step 2 In node view, right-click the controller card to reveal a shortcut menu.

Step 3 For TCC2/TCC2P/TCC3 cards, click **Reset Card** to initiate a soft reset.

For TNC/TNCE/TSC/TSCE/TNCS/TNCS-O cards, click **Soft-Reset Card** to initiate a soft reset.

Note To initiate a hard reset on the TNC/TNCE/TSC/TSCE/TNCS/TNCS-O card, right-click the card and click **Hard-Reset Card** when the card is in OOS-MT state. See Equipment Inventory for more information.

Step 4 Click **Yes** when the confirmation dialog box appears.

Step 5 Click **Close** when the “Lost connection to node, changing to Network View” dialog box appears.

Step 6 Return to node view (single-shelf mode) or multishelf view (multishelf mode) and confirm that the controller card LED is amber (standby).

Step 7 Return to your originating procedure (NTP).

DLP-G251 Resetting DWDM Cards Using CTC

Purpose	This task resets the DWDM cards using CTC.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC • NTP-G179 Installing the Transponder and Muxponder Cards
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Note The line cards normally do not need to be reset. However, you might occasionally need to reset a card for testing or as an initial trouble-clearing step. For additional information, refer to the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

Procedure

Step 1 If you will switch an active TXP or MXP card that is in a Y-cable protection group, complete the DLP-G179 Apply a Force Y-Cable or Splitter Protection Switch task. If not, continue with Step 2.

Step 2 Right-click the card that you want to reset to reveal a shortcut menu.

Step 3 Click **Reset Card**.

Step 4 Click **Yes** when the confirmation dialog box appears.

The card LED on the ONS 15454 shelf graphic will go through the following sequence: Fail (white LED), Ldg (white LED), and Act (green LED). The reset should complete within 1 to 2 minutes.

Note A software reset of the TXP and MXP card leads to removal of PM data from the PM counters. As a result, the PM counters do not display any PM data.

Step 5 If you performed a Y-cable protection group switch in Step 1, complete the DLP-G180 Clear a Manual or Force Y-Cable or Splitter Protection Switch task. If not, continue with Step 6.

Step 6 Return to your originating procedure (NTP).

NTP-G108 Viewing the Audit Trail Records

Purpose	This procedure explains how to view audit trail records. Audit trail records are useful for maintaining security, recovering lost transactions, and enforcing accountability. Accountability refers to tracing user activities; that is, associating a process or action with a specific user.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Maintenance** > **Audit** tabs.

Step 2 Click **Retrieve**.

A window containing the most recent audit trail records appears.

A definition of each column in the audit trail log is listed in the following table.

Table 4: Audit Trail Column Definitions

Column	Definition
Date	Date when the action occurred in the format MM/dd/yy HH:mm:ss
Num	Incrementing count of actions
User	User ID that initiated the action
P/F	Pass/Fail (that is, whether or not the action was executed)
Operation	Action that was taken

Left-click the column headings to display the list in ascending-to-descending or descending-to-ascending order.

Right-click the column heading to display the following options:

- Reset Sorting—Resets the column to the default setting.
- Hide Column—Hides the column from view.
- Sort Column—Sorts the table by the column’s values.
- Sort Column (incremental)—Sorts the table incrementally by multiple columns.
- Reset Columns Order/Visibility—Displays all hidden columns.
- Row Count—Provides a numerical count of log entries.

Shift-click the column heading for an incremental sort of the list.

Stop. You have completed this procedure.

NTP-G109 Off-Loading the Audit Trail Record

Purpose	This procedure describes how to off-load up to 640 audit trail log entries in a local or network drive file to maintain a record of actions performed for the node. If the audit trail log is not off-loaded, the oldest entries are overwritten after the log reaches capacity.
Tools/Equipment	None

Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click, click the **Maintenance** > **Audit** tabs.

Step 2 Click **Retrieve**.

Step 3 Click **Archive**.

Step 4 In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.

Step 5 Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 6 Click **Save**. Click **OK.**

The 640 entries are saved in this file. The next entries continue with the next number in the sequence, rather than starting over.

Note Archiving does not delete entries from the CTC audit trail log. However, entries can be self-deleted by the system after the log maximum is reached. If you archived the entries, you cannot reimport the log file back into CTC and will have to view the log in a different application.

Stop. You have completed this procedure.

NTP-G110 Off-Loading the Diagnostics File

Purpose	This procedure describes how to off-load a diagnostic file. The diagnostic file contains a set of debug commands that were run on a node and their results. This file is useful to the Cisco Technical Assistance Center (TAC) when troubleshooting problems with the node.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Maintenance or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Maintenance** > **Diagnostic** tabs.

Step 2 Click **Node Diagnostic Logs**. The Node Diagnostics dialog box is displayed.

Step 3 Click **OK** to continue.

Step 4 In the Select a Filename for the Node Diagnostics Zip Archive dialog box, navigate to the directory (local or network) where you want to save the file.

Step 5 Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is a compressed file (.zip) that can be unzipped and read by Cisco Technical Support.

Step 6 Click **Save**.

The status window shows a progress bar indicating the percentage of the file being saved.

Step 7 Click **OK**.

Stop. You have completed this procedure.

NTP-G135 Editing Network Element Defaults

Purpose	This procedure edits the factory-configured NE defaults using the NE Defaults editor. The new defaults can be applied to the node where they are edited, or exported to a file to be imported for use on other nodes. For a list of NE defaults, see the "Network Element Defaults" document.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note You can enable fast restoration of circuits by setting the NODE.circuits.FastCircuitActivation default to TRUE. This must be done for every node in the network.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Defaults** tabs. Wait for the Defaults selector frame to load the defaults. This could take several minutes.

Step 2 Under Defaults Selector, choose either a card (if editing card-level defaults) or NODE (if editing node-level defaults). Clicking on the node name (at the top of the Defaults Selector column) lists all available NE defaults (both node- and card-level) under Default Name.

Step 3 Locate a default that you want to change under Default Name.

Step 4 Click in the Default Value column for the default property that you are changing and either choose a value from the drop-down list (when available), or type in the desired new value.

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

Step 5 Click **Apply** (click in the Default Name column to activate the Apply button if it is unavailable). You can modify multiple default values before applying the changes.

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

Step 6 If you are modifying node-level defaults, a dialog box appears telling you that defaults were successfully applied to the node. Click **Yes.**

If you are modifying the IIOP Listener Port setting, a dialog box appears warning you that the node will reboot and asks if you want to continue. Click **Yes**.

Note Changes to most node defaults reprovision the node when you click Apply. Changes made to card settings using the Defaults Editor do not change the settings for cards that are already installed or slots that are preprovisioned for cards, but rather, change only cards that are installed or preprovisioned thereafter. To change settings for installed cards or preprovisioned slots, see Changing DWDM Card Settings. To change settings for transponder or muxponder cards see the chapter, Provisioning Transponder and Muxponder Cards.

Note Changing some NE defaults can cause CTC disconnection or a reboot of the node in order for the default to take effect. Before you change a default, view the Side Effects column of the Defaults editor (right-click a column header and select **Show Column** > **Side Effects**) and be prepared for the occurrence of any side effects listed for that default.

Stop. You have completed this procedure.

NTP-G136 Importing Network Element Defaults

Purpose	This procedure imports the NE defaults using the NE Defaults editor. The defaults can either be imported from the CTC software CD (factory defaults) or from a customized file exported and saved from a node. For a list of NE defaults, refer to the “Network Element Defaults” document.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Defaults** tabs.

Step 2 Click **Import**.

Step 3 If the correct file name and location of the desired file do not appear in the Import Defaults from File dialog box, click **Browse** and browse to the file that you are importing.

Step 4 When the correct file name and location appear in the dialog box, click **OK**. If you are importing the factory defaults, the correct file name is 15454-defaults.txt for ANSI shelves and 15454SDH-defaults.txt for ETSI shelves.

A pencil icon will appear next to any default value that will be changed as a result of importing the new defaults file.

Step 5 Click **Apply**.

Step 6 If the imported file fails to pass all edits, the problem field shows the first encountered problem default value that must be fixed. Change the problem default value and click **Apply**. Repeat until the imported file passes all edits successfully.

Step 7 If you are modifying node-level defaults, a dialog box appears telling you that defaults were successfully applied to the node. Click **Yes**.

Step 8 If you are modifying the IIOP Listener Port setting, a dialog box appears warning you that the node will reboot and asks if you want to continue. Click **Yes**.

Note Changes to most node defaults reprovision the node when you click **Apply**. Changes made to card settings using the Defaults Editor do not change the settings for cards that are already installed or slots that are preprovisioned for cards, but rather, change only cards that are installed or preprovisioned thereafter. To change settings for installed cards or preprovisioned slots, see Changing DWDM Card Settings. To change settings for transponder or muxponder cards, see the chapter, Provisioning Transponder and Muxponder Cards.

Note Changing some NE defaults can cause CTC disconnection or a reboot of the node in order for the default to take effect. Before you change a default, view the Side Effects column of the Defaults editor (right-click a column header and select **Show Column** > **Side Effects**) and be prepared for the occurrence of any side effects listed for that default.

Stop. You have completed this procedure.

NTP-G137 Exporting Network Element Defaults

Purpose	This procedure exports the NE defaults using the NE Defaults editor. The defaults currently displayed are exported whether or not they have been applied to the current node. The exported defaults can be imported to other nodes. For a list of NE defaults, refer to the "Network Element Defaults" document
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Defaults** editor tabs.

Step 2 Click **Export**.

Step 3 If the location where you want to export the file does not appear in the Export Defaults to File dialog box, click **Browse** and browse to the location.

Step 4 Change the file name to something that is easy to remember (the file name has no extension).

Step 5 Click **OK**.

Note The NE defaults can also be exported from the File > Export menu. These exported defaults are for reference only and cannot be imported.

Stop. You have completed this procedure.

NTP-G166 Viewing the Facilities

Purpose	This procedure displays DWDM facility information for all facilities in a node (single-shelf mode), shelf view (multishelf mode), or multishelf node (multishelf mode).
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Maintenance and higher

Procedure

Step 1 In node view (single-shelf mode), shelf view (multishelf mode), or multishelf view (multishelf mode), click the **Maintenance** > **DWDM** > **All Facilities** tabs.

- Marked—Displays a check mark if you have designated the facility for logical grouping. To mark a facility to group it with others, go to Step 2.
- Location—Displays the slot number, slot type, port number, and port type of the facility.
- Admin State—Displays the administrative state of the facility.
- Service State—Displays the service state of the facility.
- Power—Displays the power level of the facility.

Step 2 To mark certain facilities to group during column sorting, click the desired row and click **Mark**. A check mark appears in the Marked column. Click the **Marked** column header to group all of the checked facilities in ascending order. Click the **Marked** header again to sort in descending order.

Step 3 To sort the facilities by the Location, Admin State, Service State, or Power columns in ascending order, click on the desired column header. Click the column header again to sort in descending order.

Stop. You have completed this procedure.

NTP-G119 Powering Down the Node

Purpose	This procedure stops all node activity.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution The following procedure is designed to minimize traffic outages when powering down nodes, but traffic will be lost if you delete and recreate circuits that passed through a working node.

Note Always use the supplied ESD wristband when working with the Cisco ONS 15454. Plug the wristband into the ESD jack located on the fan-tray assembly or on the lower right outside edge of the shelf on the NEBS 3 shelf assembly. To access the ESD plug on the NEBS 3 shelf assembly, open the front door of the Cisco ONS 15454 chassis. The front door is grounded to prevent electrical shock. For detailed instructions on how to wear the ESD wristband, see the Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms.

Note The CTC views referenced in this procedure depend on the mode. For more information about CTC views, see CTC Operation, Information, and Shortcuts.

Procedure

Step 1 Identify the node that you want to power down. If no cards are installed, go to Step 20. If cards are installed, log into the node. See the DLP-G46 Log into CTC task for instructions.

Step 2 Choose **Go to Network View** from the View menu.

Step 3 Verify that the node is not connected to a network.

a) If the node is part of a Software R4.7 or later dense wavelength division multiplexing (DWDM) configuration, see the NTP-G130 Remove a DWDM Node and continue with Step 4.

b) If the node is not connected to a working network and the current configurations are no longer required, proceed to Step 4.

Note Before the power-down of a DWDM node, the fiber spans connected around it must be disconnected from the network. This is to prevent the accidental disconnection of wavelengths that pass through the shelf. A good indication that the shelf has been disconnected from the network is optical service channel (OSC) alarms, or no OSC channels provisioned.

Note Current configurations will be saved if Steps 4 to 20 are skipped.

Step 4 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Circuits** tab and verify that no circuits appear, then proceed to Step 5. If circuits appear, delete all the circuits that originate or terminate in the node. Complete the task, DLP-G106 Deleting Optical Channel Network Connections, DLP-G347 Deleting Optical Channel Client Connections, or DLP-G112 Deleting Overhead Circuits as needed.

Note When deleting circuits from a node, make sure that the node is not connected to any network.

Step 5 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Protection** tabs and delete all protection groups:

a) Click the protection group that needs to be deleted and click **Delete**.

b) Click **Yes**.

Repeat until no protection groups appear.

Step 6 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Comm Channels** tabs and delete all communications channel terminations:

a) Click the section data communications channel (SDCC), line data communications channel (LDCC), generic communications channel (GCC), link management protocol (LMP), provisionable (external) patchcords (PPC), or OSC termination that needs to be deleted and click **Delete**.
b) Click **Yes**.

Repeat until no SDCC, LDCC, GCC, or OSC terminations are present.

Step 7 Before deleting any installed DWDM cards, the optical sides and the optical patchcords must be deleted. In node view (single-shelf mode) or multishelf view (multishelf mode), click **Provisioning** > **WDM-ANS** > **Optical Side** tabs.

a) Select all the connections and click **Delete**.
b) Click **Yes**.

Repeat until no optical sides and the optical patchcords are present.

Step 8 In node view (single-shelf mode) or multishelf view (multishelf mode), click **Provisioning** > **WDM-ANS** > **Internal Patchcords** tabs.

a) Select all the connections and click **Delete**.
b) Click **Yes**.

Repeat until no internal patchcords are present.

Step 9 In node view (single-shelf mode) or multishelf view (multishelf mode), click **Provisioning** > **WDM-ANS** > **Provisioning** tabs and delete all the ANS parameters.

a) Select all the ANS parameters and click **Remove**. The Network Type parameter cannot be deleted.
b) Click **Yes**.

Step 10 In node view (single-shelf mode) or multishelf view (multishelf mode), click **Provisioning** > **WDM-ANS** > **Passive Cards** tabs, and delete all the passive cards.

a) Click the passive card you want to delete.
b) Click **Delete**, then click **Yes**.

Step 11 Repeat Step a and Step b for each installed passive card.

Step 12 For each installed channel-bearing card , make sure all lines and bands are not in IS-NR (ANSI) or Unlocked-Enabled (ETSI) service state:

a) In card view, click the **Provisioning** > **Optical Line** > **Parameters** tabs.
b) In the Admin State column for each line, make sure that the default state IS, AINS (ANSI), or Unlocked,automaticInservice (ETSI) is selected.
c) Click the **Provisioning** > **Optical Chn** > **Parameters** tabs.
d) In the Admin State column for each line, make sure that the default state IS, AINS (ANSI), or Unlocked,automaticInservice (ETSI) is selected.

Step 13 For each installed DWDM band-bearing card , make sure all lines and bands are not in the IS-NR (ANSI) or Unlocked-Enabled (ETSI) service state:

a) In card view, click the **Provisioning** > **Optical Line** > **Parameters** tabs.
b) In the Admin State column for each line, make sure that the default state IS, AINS (ANSI), or Unlocked,automaticInservice (ETSI) is selected.

c) Click the **Provisioning** > **Optical Band** > **Parameters** tabs.

d) In the Admin State column for each line, make sure that the default state IS, AINS (ANSI), or Unlocked,automaticInservice (ETSI) is selected.

Step 14 For each installed DWDM card, make sure all lines are not in the IS-NR (ANSI) or Unlocked-enabled (ETSI) service state:

a) In card view, click the appropriate tab depending on the card:

For MXP_2.5G, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_10E, click the **Provisioning** > **Line** > **SONET** tabs if the card was provisioned for a SONET payload, or the **Provisioning** > **Line** > **SDH** tabs if the card was provisioned for an SDH payload.

For TXP_MR_2.5G, TXPP_MR_2.5G, and MXPP_MR_2.5G cards, click the **Provisioning** > **Line** > **SONET** tabs.

For MXP_2.5G_10E cards, click the **Provisioning** > **Line** > **Trunk** tabs.

For MXP_MR_2.5G cards, click the **Provisioning** > **Line** > **Client** tabs.

For ADM-10G, OTU2_XP, 40E-TXP-C, 40ME-TXP-C, 40G-MXP-C, 40E-MXP-C, 40ME-MXP-C, 100G-LC-C, 10x10G-LC, CFP-LC, 100G-CK-C, 100GS-CK-LC, 200G-CK-LC cards, click the **Provisioning** > **Line** > **Ports** tabs.

For 32MUX-O, 32DMX-0, 32DMX, 32WSS, 40MUX, 40DMUX-C, TDC-CC, TDC-FC, OPT-BST, OPT-PRE cards, click the **Provisioning** > **Optical Line** > **Parameters** tabs.

For 32DMX, 32DMX-0, 40-DMX-C, 40-MUX-C, 40-DMX-CE, 4MD cards, click the **Provisioning** > **Optical Chn** > **Parameters** tabs.

For 40-WSS-C/40-WSS-CE cards, click the **Provisioning** > **Optical Chn: Optical Connector** > **x** > **Parameters** tabs.

For 40-WXC-C cards, click the **Provisioning** > **WXC Line** > **Parameters** tabs.

For 40-DMX-C, 40-MUX-C, and 40-DMX-CE cards, click the **Provisioning** > **Optical Line** > **Parameters** tabs.

For 4MD-xx.x cards, click the **Provisioning** > **Optical Band** > **Parameters** tabs.

For GE_XP, 10GE_XP, GE_XPE, and 10GE_XPE cards, click the **Provisioning** > **Ether Ports** > **Ports** tabs.

For OPT-BST and OPT-PRE cards, click the **Provisioning** > **Optical Ampli Line** > **Parameters** tabs.

For the 40-SMR1-C and 40-SMR2-C cards, click the **Provisioning** > **Optical Line** > **Parameters** tabs and **Provisioning** > **Opt. Ampli. Line** > **Parameters** tabs.

For OSC-CSM and OSCM cards, click the **Provisioning** > **Optical Line** > **Parameters** tabs.

For ADM_10G cards, click the **Provisioning** > **Line** > **Ports** tabs.

b) In the Admin State column for each line, make sure that the default state IS, AINS (ANSI) or Unlocked,automaticInservice (ETSI) is selected.

c) Repeat Steps a and b for each installed DWDM card.

Note Ports are put in service when circuits are provisioned, and put out of service when circuits are deleted. When circuits are deleted the Admin State displays as IS, AINS (ANSI) or Unlocked,automaticInservice (ETSI) and the Service State displays OOS-AU,AINS (ANSI) or Unlocked-disabled,automaticInService (ETSI).

Step 15 Remove all fiber connections to the cards.

Step 16 In node view (single-shelf mode) or shelf view (multishelf mode), right-click an installed card and click **Delete**.

Step 17 Click **Yes**.

Step 18 After you have deleted the card, open the card ejectors and remove it from the node.

Step 19 Repeat Step 15 through Step 18 for each installed card.

Note

- You cannot delete a TCC2/TCC2P/TCC3 card in Cisco Transport Controller (CTC). Physically remove it after all the other cards have been deleted and removed.
- Due to memory limitations, TCC2/TCC2P cards are not supported from Release 10.5.2 onwards. As a result, in a multishelf configuration, the TCC2/TCC2P card cannot be a node controller or a shelf controller. Upgrade the TCC2/TCC2P card to a TCC3 card.

Note You cannot delete an active TNC/TNCE/TSC/TSCE/TNCS/TNCS-O card in Cisco Transport Controller (CTC). Physically remove it after all the other cards have been deleted and removed.

Step 20 Shut off the power from the power supply that feeds the node.

Step 21 Disconnect the node from its external fuse source.

Step 22 Store all of the cards that you removed and update inventory records according to local site practice.

Stop. You have completed this procedure.

NTP-G356 Verify Connections in Optical Cables

Purpose	This task verifies the optical interconnection between the optical cards inside the Flex ROADM.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC Connection Verification Pre-Requisites
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view (single-shelf mode), click the **Maintenance** > **DWDM** > **Connection Verification** tabs to retrieve connection information. The following information is displayed in the pane:

- Attribute:

- From—Displays the originating slot for connection verification.
- To—Displays the destination slot for connection verification.
- Connectivity Verification—Displays connectivity status. This information is summarized and displayed only for the MPO cable and not for each of the patch cords in it. The different status include:
    - Connected—Cable or patchcord is connected.
    - Not Connected—Cable or patchcord is disconnected.

      In this state the corresponding row is highlighted in orange.
    - Disabled—Cable or patchcord is excluded from connection verification.
    - Not Measurable—Power source not detected; cable or patchcord cannot be tested for connection verification.
    - Not Verified—Cable or patchcord is yet to be tested for connection verification (this is the default status at first boot).
- Connectivity Last Change—Displays the date and time when the connectivity information was previously changed.
- Insertion Loss Verification—Displays insertion loss verification status that is one of the following:
    - Not Verified—Cable or patchcord is yet to be tested for insertion loss verification (this is the default status at first boot).
    - Not Measurable—Power source not detected; cable or patchcord cannot be tested for insertion loss verification.
    - Loss OK—Cable or patchcord insertion loss is within expected value.
    - Degrade—Cable or patchcord insertion loss is degrading.

      When the Insertion Loss is greater than the Insertion Loss Degrade Threshold and less than the Insertion Loss Fail Threshold, the Insertion Loss Verification of the patch cord is Degrade. The corresponding row of the patch cord in the Connection Verification pane is highlighted in yellow.
    - Fail—Cable or patchcord insertion loss crossed the fail threshold. When this condition occurs, the patchcord is highlighted in the GUI to indicate the Fail condition.

      When the Insertion Loss is greater than the Insertion Loss Fail Threshold, the Insertion Loss Verification of the patch cord is Fail. The corresponding row of the patch cord in the Connection Verification pane is highlighted in orange.
    - Disabled—Cable or patchcord is excluded from connection verification.
- Insertion Loss Last Change—Displays the date and time when the insertion loss verification information was previously changed.
- Excess Insertion Loss [dB]—Displays the excess loss versus the maximum specified loss for the cable under test. When the shelf controller reboots, the information in Excess Insertion Loss column is lost. If a chain icon appears next to the excess insertion loss value, it indicates that two or more

patch cords are considered as a chain from the connection verification point of view. You can right-click the patch cord and click **Troubleshooting** to view the details of the linked patch cords.

- Last Run—Displays the date and time when the connection verification and insertion loss verification was run previously. When the shelf controller reboots, the information in Last Run column is lost.
- Ack—Displays the Alarm Acknowledgment information for a specific fiber.

Step 2 To refresh the connection verification information, click **Refresh.**

Step 3 Click **Enable Verifications** to enable or disable the connection verification at the node level.

Step 4 Perform one of the steps that follow:

- Click **Connectivity Check** to perform connection verification on all the patchcords and MPO cables. With MPO cables, the connectivity check is performed only on a sub-set of fibers.

OR

- Click **Loss Verification** to perform the insertion loss verification on all the patchcords and MPO cables.

The IPC-Verification-Running condition is raised when connection or insertion loss verification is launched. To disable this condition, click **Provisioning > Defaults** tabs. In the **Node Defaults** area, click patchcordverification in the **Defaults Selector**, and configure the NODE.patchcords.Verification.raiseRaisingCondition as FALSE. The default values of NODE.patchcords.Verification.thresholdFail (Insertion Loss Fail Threshold) and NODE.patchcords.Verification.thresholdDegrade (Insertion Loss Degrade Threshold) parameters are 4 dB and 1.5 dB respectively. These two default thresholds are used to generate the alarms.

A progress bar appears when you launch connection or insertion loss verification. You can click **Abort** to stop the connection or insertion loss verification at any point. During the verification process, you can view the number of patch cords that have been verified and the total number of patch cords to be verified.

Step 5 After connection verification, perform the relevant set of steps:

- If the Insertion Loss Verification results for a patchcord are Fail or Degrade, carry out this set of steps:

  a. Remove the patchcord.

  b. Clean the patch cord.

  c. Install the patchcord.

  d. Perform Step 4 (Insertion Loss Verification) again.

- If the patchcord status is Not Connected, it raises the IPC-VERIFICATION-FAIL alarm on the node. To clear this condition, carry out this set of steps:

  a. Ensure the patchcords are installed correctly on both the ends.

  b. Perform Step 4 (Insertion Loss Verification) again.

  c. Replace the patchcords if the alarm still exist.

- If the IPC-LOOPBACK-MISS alarm is raised on any port, carry out this set of steps to clear this condition:

  a. Identify the port with IPC-LOOPBACK-MISS alarm.

  b. Check if the loopback is installed on the port.

c. If the loopback is installed correct, perform Step 4 (Insertion Loss Verification) again.

d. Replace the loopback if the alarm still exists.

Step 6 Double click the MPO cable to see the information applicable to individual fibers.

Step 7 When you right click an MPO cable or a single patchcord, a context menu appears with the options listed in the following table.

Table 5: Side View Context Menu Options

Option	Description
Verify Loss and Connectivity	Performs insertion loss verification on selected MPO cables or patch cords.
Enable Verifications	Enables connection verification on selected MPO cables or patch cords.
Disable Verifications	Disables connection verification on selected MPO cables or patch cords.
Acknowledge Loss Alarm	Allows MPO cable or patch cord to operate beyond the insertion loss thresholds without raising an alarm. Acknowledges the Insertion Loss Verification result related to the selected MPO cables or patchcords. If all the IL Verification problems on the current node are acknowledged the consequent alarm on the Node is cleared.
Clear Acknowledge	Clears the acknowledgment on the selected MPO cable or patchcord. The Insertion loss verification result becomes Fail or Degrade. This operation can raise the IPC-VERIFICATION-FAIL or IPC-VERIFICATION-DEGRADE alarm on the node.
Troubleshooting	Launches the **Excess Loss** dialog box and allows you to view and troubleshoot the patch cords that have an excess insertion loss that is higher than the set threshold. You can view the originating and destination slots for the connection verification. You can view the patch cords in the Cable View and Front Panel View of the Card. The selected patch cord is highlighted in black. You can perform the following steps: **a.** Remove the patchcord. **b.** Clean the patch cord. **c.** Install the patchcord. **d.** Perform Step 4 (Insertion Loss Verification) again.

Step 8 **Stop. You have completed this procedure.**

What to do next

Alarm Behavior

- If there is at least one patch cord is highlighted in yellow and no patch cords highlighted in orange on a node, an IPC-VERIFICATION-DEGRADE alarm is raised on the node.
- If there is at least one patch cord is highlighted in orange on the node, an IPC-VERIFICATION-FAIL alarm is raised on the node. An IPC-VERIFICATION-FAIL alarm clears a previously raised IPC-VERIFICATION-DEGRADE alarm.