



## Maintain the Node

---

This chapter provides procedures for maintaining the Cisco ONS 15454.

### Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary for general troubleshooting information and alarm or error descriptions.

This section lists the chapter procedures (NTPs). Turn to a procedure to view its tasks (DLPs).

1. [NTP-A107 Inspect, Clean, and Replace the Air Filter, page 15-2](#)—Complete as needed.
2. [NTP-A108 Back Up the Database, page 15-4](#)—Complete as needed.
3. [NTP-A109 Restore the Database, page 15-5](#)—Complete as needed.
4. [NTP-A320 View and Manage OSI Information, page 15-8](#)—Complete as needed.
5. [NTP-A163 Restore the Node to Factory Configuration, page 15-9](#)—Complete as needed to clear the database and upload a blank database and the latest software.
6. [NTP-A300 Viewing the Audit Trail Records, page 15-10](#)—Complete as needed.
7. [NTP-A214 Off-Load the Audit Trail Record, page 15-12](#)—Complete as needed.
8. [NTP-A306 Off-Load the Diagnostics File, page 15-13](#)—Complete as needed.
9. [NTP-A302 Initiate or Clear an External Switching Command, page 15-13](#)—Complete as needed to initiate Force switches, Manual switches, lock-ons, and lockouts.
10. [NTP-A112 Clean Fiber Connectors, page 15-14](#)—Complete as needed.
11. [NTP-A332 Reset a Card in CTC, page 15-15](#)—Complete as needed.
12. [NTP-A215 View G-Series Ethernet Maintenance Information, page 15-16](#)—Complete as needed.
13. [NTP-A239 View E-Series Ethernet Maintenance Information, page 15-17](#)—Complete as needed.
14. [NTP-A218 Change the Node Timing Reference, page 15-17](#)—Complete as needed.
15. [NTP-A223 View the ONS 15454 Timing Report, page 15-18](#)—Complete as needed.
16. [NTP-A287 Replace an In-Service Cross-Connect Card, page 15-21](#)—Complete as needed.
17. [NTP-A288 Replace the Fan-Tray Assembly, page 15-22](#)—Complete as needed.
18. [NTP-A290 Replace the Alarm Interface Panel, page 15-26](#)—Complete as needed.
19. [NTP-A291 Replace the Plastic Lower Backplane Cover, page 15-31](#)—Complete as needed.

20. [NTP-A162 Replace the UBIC-V EIA, page 15-33](#)—Complete as needed.
21. [NTP-A336 Edit Network Element Defaults, page 15-35](#)—Complete as needed to edit the factory-configured (default) network element settings for the Cisco ONS 15454.
22. [NTP-A337 Import Network Element Defaults, page 15-37](#)—Complete as needed to import the factory-configured (default) network element settings for the Cisco ONS 15454.
23. [NTP-A338 Export Network Element Defaults, page 15-38](#)—Complete as needed to export the factory-configured (default) network element settings for the Cisco ONS 15454.

## NTP-A107 Inspect, Clean, and Replace the Air Filter

<b>Purpose</b>	This procedure ensures that the air filter is free from dirt and dust, which allows optimum air flow and prevents dirt and dust from entering the shelf.
<b>Tools/Equipment</b>	New air spare filter and pinned hex key tool
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



### 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 air filters are single-use only. They must not be cleaned and reused. This is a Telcordia NEBS requirement, GR-63-CORE Issue 4.



### Note

Air filters must be inspected every month. If they are dirty or clogged with dust, they must be replaced with a new air filter.



### Note

Although the filter can work if it is installed with either side facing up, it is recommended that you install it with the metal bracing facing up to preserve the surface of the filter.

### Step 1

If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that might have collected on the filter and proceed to [Step 8](#). [Figure 15-1](#) illustrates a fan-tray air filter in an external filter bracket.

### Step 2

If the filter is installed below the fan tray and not in the external filter brackets, open the front door of the shelf assembly using the following substeps. If the front door is already open, proceed to [Step 3](#).

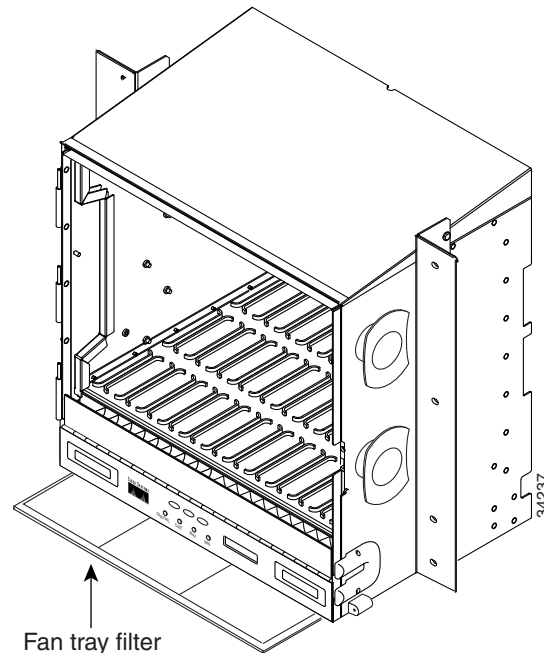
- a. Open the front door lock.

The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

- b. Press the door button to release the latch.

- c. Swing the door open.
- Step 3** Remove the front door (optional). If you do not want to remove the door or it is already removed, proceed to [Step 4](#).
- a. Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
  - b. Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
  - c. Secure the dangling end of the ground strap to the door or chassis with tape.

**Figure 15-1** ANSI Shelf Fan-Tray Air Filter in an External Filter Bracket (Front Door Removed)



- Step 4** Push the outer side of the handles on the fan-tray assembly to expose the handles.
- Step 5** Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.
- Step 6** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.
- Step 7** Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that might have collected on the filter.
- Step 8** Visually inspect the air filter material for dirt and dust.
- Step 9** Replace the air filter with a new one if the air filter is dirty or clogged with dust.



**Caution**

Do not leave the fan tray out of the chassis for an extended period of time because excessive heat can damage the ONS 15454 cards.

- Step 10** Replace the clean filter:
- a. If the air filter is installed in the external filter brackets, slide the dry air filter all the way to the back of the brackets to complete the procedure.

- b. If the filter is installed below the fan-tray assembly, slide the dry/clean air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.

**Caution**

If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the filter until the fan tray fits correctly.

**Note**

On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

- Step 11** To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.
- Step 12** Rotate the retractable handles back into their compartments.
- Step 13** If you replace the door, also reattach the ground strap.
- Step 14** Close and lock the door.
- Step 15** Return to your originating procedure (NTP).

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

## NTP-A108 Back Up the Database

<b>Purpose</b>	This procedure stores a backup version of the TCC2/TCC2P (software) database on the workstation running Cisco Transport Controller (CTC) or on a network server.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required. Cisco recommends performing a database backup at approximately weekly intervals and prior to and after configuration changes.
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Maintenance or higher

**Note**

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

**Note**

The following parameters are not backed up and restored: node name, and Internet Inter-ORB Protocol (IOP) port. If you change the node name and then restore a backed up database with a different node name, the circuits map to the new node name. Cisco recommends keeping a record of the old and new node names.

- 
- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67 at the node you want to back up. If you are already logged in, continue with [Step 2](#).
- Step 2** Click the **Maintenance > Database** tabs.
- Step 3** Click **Backup**.
- Step 4** 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 5** Click **Save**.
- Step 6** Click **OK** in the confirmation dialog box.
- Stop. You have completed this procedure.**
- 

## NTP-A109 Restore the Database

<b>Purpose</b>	This procedure restores the TCC2/TCC2P software database.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A108 Back Up the Database, page 15-4</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser



### Caution

E1000-2 cards lose traffic for approximately 90 seconds when an ONS 15454 database is restored. Traffic is lost during the period of spanning tree reconvergence. The CARLOSS alarm appears and clears during this period.



### Caution

If you are restoring the database on multiple nodes, wait approximately one minute after the TCC2/TCC2P reboot has completed on each node before proceeding to the next node.



### Caution

TCC2P cards can be used in single IP address (repeater) and dual IP address (secure) modes. The secure mode has advanced features that affect database restore. A database from a secure node cannot be loaded on an unsecure repeater node. An unsecure repeater node database can be loaded onto a secure node but the database will follow the node characteristics (that is, become secure). A secure database cannot be loaded onto a TCC2; only TCC2P cards support secure mode. For more information about the dual IP-address secure mode, see the “[NTP-A169 Set Up CTC Network Access](#)” procedure on page 4-7. Also refer to the “Management Network Connectivity” chapter in the *Cisco ONS 15454 Reference Manual*.



### Caution

To avoid a node IP and secure IP ending up in the same domain after restoring a database, ensure that the node IP stored in the database differs in domain from that of the node in repeater mode. Also, after restoring a database, ensure that the node IP and secure IP differ in domain.

**Note**

The following parameters are not backed up and restored: node name, and IIOP port. If you change the node name and then restore a backed up database with a different node name, the circuits map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

**Note**

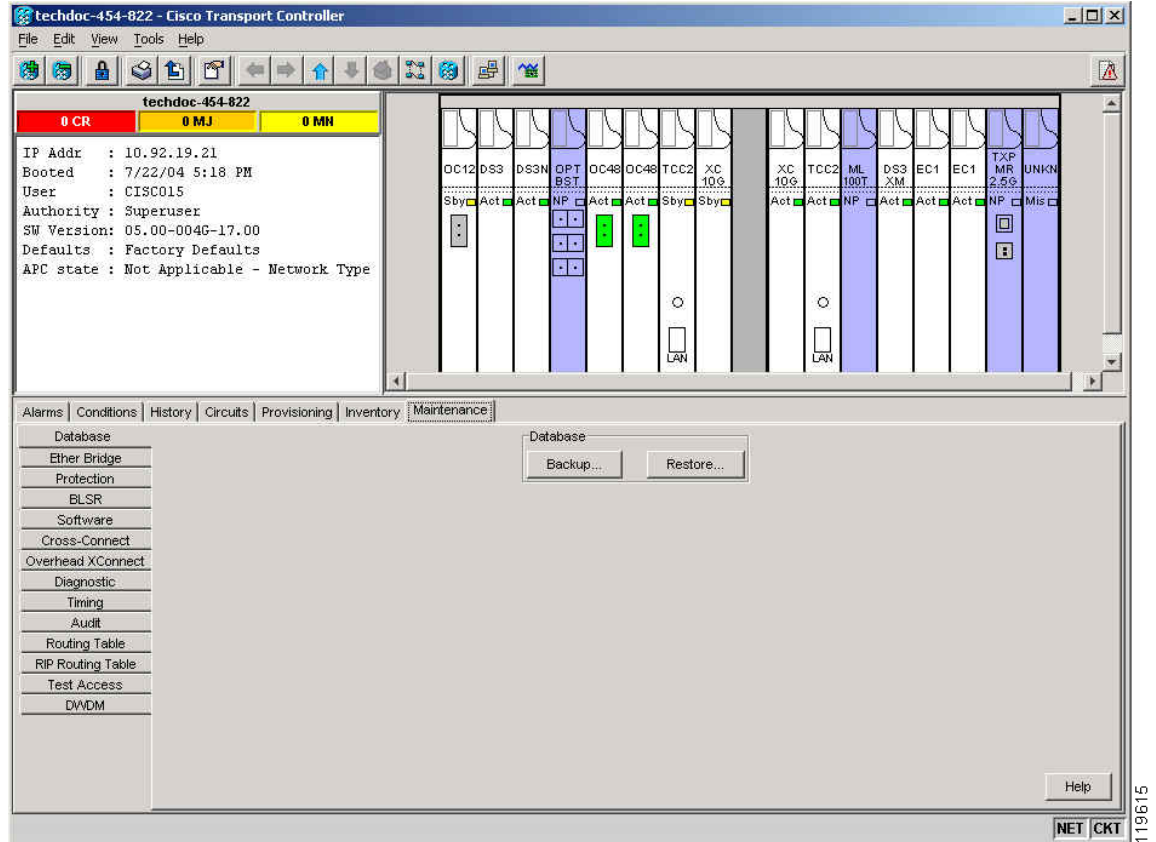
ML-Series Ethernet cards must be reset after a database restore. For more information about restoring these cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

**Note**

If you want to revert to a previously used software load, consult the platform-specific upgrade documentation for instructions.

- 
- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67 at the node where you are restoring the database. If you are already logged in, continue with Step 2.
- Step 2** Ensure that no BLSR switch events are present; for example, ring-switch east or west. In network view, click the **Conditions** tab and click **Retrieve** to view a list of conditions.
- Step 3** If switch events need to be cleared, in node view click the **Maintenance > BLSR** tabs and view the West Switch and East Switch columns.
- If a switch event (not caused by a line failure) is present, choose **CLEAR** from the drop-down list and click **Apply**.
  - If a switch event caused by the Wait to Restore (WTR) condition is present, choose **CLEAR** from the drop-down list and click **Apply**.
- When a switch event is cleared, NO COMMAND appears in the column to indicate that the switch event is no longer in effect.
- Step 4** In node view, click the **Maintenance > Database** tabs. [Figure 15-2](#) shows this tab for the TCC2 card. (The TCC2P tab is similar.)

Figure 15-2 Restoring the TCC2 Database



**Step 5** Click **Restore**.

**Step 6** 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 ONS 15454 software CD.

**Step 7** Click the database file to highlight it.

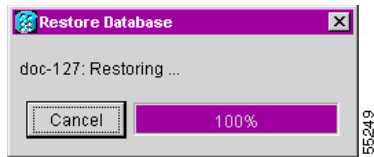
**Step 8** Click **Open**. The DB Restore dialog box appears.



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

**Step 9** Click **Restore**.

The Restore Database dialog box monitors the file transfer (Figure 15-3).

**Figure 15-3 Restoring the Database—In-Process Notification**

- Step 10** Wait for the file to complete the transfer to the TCC2/TCC2P card.
- Step 11** Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears. Wait for the node to reconnect.
- Step 12** If you cleared a switch in [Step 3](#), reapply the switch as needed.
- Stop. You have completed this procedure.**

## NTP-A320 View and Manage OSI Information

<b>Purpose</b>	This procedure allows you to view and manage OSI including the ES-IS and IS-IS routing information tables, TARP data cache and manual area table.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A108 Back Up the Database, page 15-4</a> <a href="#">NTP-A260 Set Up Computer for CTC, page 3-1</a> <a href="#">NTP-A318 Provision OSI, page 4-14</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

**Note**

Additional information about the ONS 15454 implementation of OSI is provided in the “Management Network Connectivity” chapter of the *Cisco ONS 15454 Reference Manual*.

- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67. If you are already logged in, continue with Step 2.
- Step 2** Perform any of the following tasks as needed:
- [DLP-A549 View IS-IS Routing Information Base, page 22-53](#)
  - [DLP-A550 View ES-IS Routing Information Base, page 22-54](#)
  - [DLP-A551 Manage the TARP Data Cache, page 22-54](#)
- Stop. You have completed this procedure.**



# NTP-A163 Restore the Node to Factory Configuration

<b>Purpose</b>	This procedure reinitializes the ONS 15454 using the CTC reinitialization tool. Reinitialization uploads a new software package to the TCC2/TCC2P cards, clears the node database, and restores the factory default parameters.
<b>Tools/Equipment</b>	ONS 15454 SONET System Software CD, Version 7.2  JRE 1.4.2 or JRE 5.0 must be installed on the computer 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 5.0.
<b>Prerequisite Procedures</b>	<a href="#">NTP-A108 Back Up the Database, page 15-4</a> <a href="#">NTP-A260 Set Up Computer for CTC, page 3-1</a>  One of the following: <ul style="list-style-type: none"> <li>• <a href="#">NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-3, or</a></li> <li>• <a href="#">NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-5</a></li> </ul>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Superuser



## Caution

Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinit 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

The following parameters are not backed up and restored when you delete the database and restore the factory settings: node name, IP address, subnet mask and gateway, and IIOP port. If you change the node name and then restore a backed up database with a different node name, the circuits map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

**Step 1** If you need to install or replace one or more TCC2/TCC2P cards, see the “[DLP-A36 Install the TCC2/TCC2P Cards](#)” task on page 17-42.

**Step 2** If you are using Microsoft Windows, complete the “[DLP-A244 Use the Reinitialization Tool to Clear the Database and Upload Software \(Windows\)](#)” task on page 19-24.

**Step 3** If you are using UNIX, complete the “[DLP-A245 Use the Reinitialization Tool to Clear the Database and Upload Software \(UNIX\)](#)” task on page 19-26.

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

---

## NTP-A300 Viewing the Audit Trail Records

<b>Purpose</b>	This procedure describes 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.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

**Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67 at the node where you want to view the audit trail log. If you are already logged in, continue with [Step 2](#).

**Step 2** In the node view, click the **Maintenance > Audit** tabs.

**Step 3** Click **Retrieve**.

A window containing the most recent Audit Trail records appears as shown in [Figure 15-4](#).

Figure 15-4 Viewing the Audit Trail Records

techdoc-454-822 - Cisco Transport Controller

File Edit View Tools Help

techdoc-454-822

0 CR 0 MJ 0 MH

IP Addr : 10.92.19.21  
 Booted : 7/22/04 5:18 PM  
 User : CISCO15  
 Authority : Superuser  
 SW Version: 05.00-004G-17.00  
 Defaults : Factory Defaults  
 APC state : Not Applicable - Network Type

Database	Date	Num	User	P/F	Operation
Ether Bridge	06/01/04 02:48:14	161	CISC...	P	Event:EventManager::RegisterClient("64.101.146.179:EventReceiver", "IOR:00000000000001e49444c3a43b6")
Protection	06/01/04 02:48:05	160	ICOR...	P	Security::General::login("CISCO15", "64.101.146.179", "64.101.146.179", "SUCCESS")
BLSR	06/01/04 02:23:35	159	CISC...	P	Event:EventManager::RegisterClient("192.168.1.100:EventReceiver", "IOR:00000000000001e49444c3a43b6")
Software	06/01/04 02:23:24	158	ICOR...	P	Security::General::login("CISCO15", "192.168.1.100", "192.168.1.100", "SUCCESS")
Cross-Connect	06/01/04 01:40:22	157	ICOR...	X	Security::General::logout()
Overhead XConnect	06/01/04 01:40:22	156	CISC...	P	Security::General::logout("CISCO15", "64.101.146.179", "*****")
Diagnostic	06/01/04 01:04:06	155	CISC...	P	Equipment::EntityTable::provisionModule(SLOT-4, E1000_CARD)
Timing	06/01/04 01:03:59	154	CISC...	P	Equipment::Module::unprovision(SLOT-4)
Audit	06/01/04 01:02:42	153	CISC...	P	If::General::setAdminState(X= 0x004002, ADMIN_JS, FAC-4-1)
Routing Table	06/01/04 01:02:42	152	CISC...	P	EtherMedia::General::setGmacLineAdminInfo(X= 0x004002)
RIP Routing Table	06/01/04 01:02:42	151	CISC...	P	EtherMedia::General::setGmacLineAdminInfo(X= 0x004002)
Test Access	06/01/04 01:02:16	150	CISC...	P	EtherMedia::General::setGmacLineAdminInfo(X= 0x004002)
Test Access	06/01/04 01:02:16	149	CISC...	P	EtherMedia::General::setGmacLineAdminInfo(X= 0x004002)
DWDM	06/01/04 01:02:16	148	CISC...	P	If::General::setAdminState(X= 0x004002, ADMIN_OOS_MT, FAC-4-1)
DWDM	06/01/04 01:01:41	147	CISC...	P	Equipment::EntityTable::provisionModule(SLOT-4, G1000_CARD)

Retrieved: July 26, 2004 2:09:52 PM CDT

A definition of each column in the Audit Trail log is listed in Table 15-1.

Table 15-1 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

- Step 4** Right-click on the column headings to display the list in ascending-to-descending or descending-to-ascending order.
- Step 5** Left-click on the column heading to display the following options:
- Reset Sorting—Resets the column to the default setting.
  - Hide Column—Hides the column from view.
  - Reset Columns Order/Visibility—Displays all hidden columns.
  - Row Count—Provides a numerical count of log entries.
- Step 6** Shift-click on the column heading for an incremental sort of the list.

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

---

## NTP-A214 Off-Load the Audit Trail Record

<b>Purpose</b>	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.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67 at the node where you want to off-load the audit trail log. If you are already logged in, continue with [Step 2](#).
- Step 2** In the node view, click the **Maintenance > Audit** tabs.
- Step 3** Click **Retrieve**.
- Step 4** Click **Archive**.
- Step 5** In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.
- Step 6** 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 7** Click **Save**.
- 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-A306 Off-Load the Diagnostics File

<b>Purpose</b>	This task describes how to off-load a diagnostic file. The diagnostic file contains a set of debug commands run on a node and its results. This file is useful to Cisco Technical Support (TAC) when troubleshooting problems with the node.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Maintenance or higher

- 
- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67 at the node where you want to off-load the diagnostics file. If you are already logged in, continue with [Step 2](#).
- Step 2** In the node view, click the **Maintenance > Diagnostic** tabs.
- Step 3** Click the **Retrieve Tech Support Log**.
- Step 4** In the Saving Diagnostic File 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 (.gzip) that can be unzipped and read by Cisco Technical Support.
- Step 6** Click **Save**.
- The Get Diagnostics status window shows a progress bar indicating the percentage of the file being saved, then shows “Get Diagnostics Complete.”
- Step 7** Click **OK**.
- Stop. You have completed this procedure.**
- 

## NTP-A302 Initiate or Clear an External Switching Command

<b>Purpose</b>	This procedure describes how to apply an external switching command to an optical or electrical card, including Manual and Force switches and lock-ons and lockouts.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A324 Create Protection Groups</a> , page 4-10
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Superuser

- 
- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67.

- Step 2** As needed, complete the “[DLP-A365 Initiate an Optical Protection Switch](#)” task on page 20-48.
- Step 3** As needed, complete the “[DLP-A366 Initiate an Electrical Protection Switch](#)” task on page 20-49.
- Step 4** To prevent traffic on a working or protect card from switching to the other card in the pair, complete the “[DLP-A201 Apply a Lock-on](#)” task on page 19-1.
- Step 5** To prevent traffic from switching to the protect card, complete the “[DLP-A202 Apply a Lockout](#)” task on page 19-2.




---

**Note** A combination of lock-on and lockout is allowed in 1:1 and 1:N protection; for example, a lock-on on the working card and a lockout on the protect card is permissible.

---

- Step 6** To remove a lock-on or lockout and return a protection group to its usual switching method, complete the “[DLP-A203 Clear a Lock-on or Lockout](#)” task on page 19-3.




---

**Note** A non-alarmed event (INHSW) is raised when a card is placed in a Lock On or Lock Out state.

---

- Step 7** To lock out a span on a BLSR, which prevents traffic from switching to the locked out span, complete the “[DLP-A299 Initiate a BLSR Span Lockout](#)” task on page 19-61.
- Step 8** As needed, complete the “[DLP-A300 Clear a BLSR Span Lockout](#)” task on page 20-1.
- Step 9** As needed, complete the “[DLP-A301 Initiate a BLSR Manual Ring Switch](#)” task on page 20-2.
- Step 10** As needed, complete the “[DLP-A241 Clear a BLSR Manual Ring Switch](#)” task on page 19-22.
- Step 11** As needed, complete the “[DLP-A303 Initiate a BLSR Force Ring Switch](#)” task on page 20-3.
- Step 12** As needed, complete the “[DLP-A194 Clear a BLSR Force Ring Switch](#)” task on page 18-62.
- Step 13** As needed, complete the “[DLP-A197 Initiate a Path Protection Force Switch](#)” task on page 18-64.
- Step 14** As needed, complete the “[DLP-A198 Clear a Path Protection Force Switch](#)” task on page 18-65.

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

---

## NTP-A112 Clean Fiber Connectors

<b>Purpose</b>	This procedure cleans the fiber connectors.
<b>Tools/Equipment</b>	Inspection microscope Type A Fiber Optic Connector Cleaner (CLETOP reel) Optical swab Optical receiver cleaning stick
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

**Warning**

**Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

**Step 1** Using an inspection microscope, inspect each fiber connector for dirt, cracks, or scratches.

**Step 2** Replace any damaged fiber connectors.



**Note** Replace all dust caps whenever the equipment is unused for 30 minutes or more.

**Step 3** Complete the “[DLP-A205 Clean Fiber Connectors with CLETOP](#)” task on page 19-4 as necessary.

**Step 4** Complete the “[DLP-A206 Clean the Fiber Adapters](#)” task on page 19-4 as necessary.

**Note**

To clean multi-fiber optic connectors, complete the “[A204 Clean Multi Fiber-Optic Cable Connectors](#)” alarm on page 19-3 as necessary.

**Caution**

Do not reuse optical swabs. Keep unused swabs off of work surfaces.

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

## NTP-A332 Reset a Card in CTC

<b>Purpose</b>	This procedure resets cards in CTC.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A36 Install the TCC2/TCC2P Cards, page 17-42</a> <a href="#">NTP-A16 Install Optical Cards and Connectors, page 2-7</a> <a href="#">NTP-A17 Install the Electrical Cards, page 2-10</a> <a href="#">NTP-A246 Install Ethernet Cards and Connectors, page 2-11</a> <a href="#">NTP-A274 Install the FC_MR-4 Card, page 2-13</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser

**Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67. If you are already logged in, continue with Step 2.

**Step 2** As necessary, complete the “[DLP-A364 Reset the TCC2/TCC2P Card Using CTC](#)” task on page 20-48.

- Step 3** To reset an optical, electrical, E-Series Ethernet, G-Series Ethernet, ML-Series Ethernet, CE-1000-4 Ethernet, or Storage Access Networking (SAN) cards, complete the [“DLP-A460 Reset a Traffic Card Using CTC” task on page 21-43](#).
- Step 4** As necessary complete the [“DLP-A54 Hard-Reset a CE-100T-8 Card Using CTC” task on page 17-64](#).
- Step 5** As necessary, complete the [“DLP-A224 Soft-Reset a CE-100T-8 Card Using CTC” task on page 19-16](#).
- Stop. You have completed this procedure.**
- 

## NTP-A215 View G-Series Ethernet Maintenance Information

<b>Purpose</b>	This procedure enables you to view loopback, bandwidth, and J1 path trace information for G-Series Ethernet cards.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A246 Install Ethernet Cards and Connectors, page 2-11</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

- Step 1** Complete the [“DLP-A60 Log into CTC” task on page 17-67](#). If you are already logged in, continue with [Step 2](#).
- Step 2** In node view, double-click a G-Series Ethernet card. The card view appears.
- Step 3** To view loopback status, click the **Maintenance > Loopback** tabs.  
The Port and Service State columns identify the port number and current service state (In-Service and Normal [IS-NR], Out-of-Service and Management, Disabled [OOS-MA,DSBLD], or Out-of-Service and Management, Maintenance [OOS-MA,MT]) for each port. The Loopback Type column identifies the type of loopback (None, Terminal [Inward], or Facility [Line]) applied to each port on the card.
- Step 4** To view Ethernet bandwidth utilization, click the **Maintenance > Bandwidth** tabs.
- Step 5** Click **Retrieve Bandwidth Usage**.  
The current STS bandwidth usage information appears.
- Step 6** To view J1 path trace information, click the **Maintenance > Path Trace** tabs and then click **Retrieve**.
- Stop. You have completed this procedure.**
-



## NTP-A239 View E-Series Ethernet Maintenance Information

<b>Purpose</b>	This procedure enables you to view maintenance information for E-Series Ethernet cards.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A246 Install Ethernet Cards and Connectors, page 2-11</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher



**Note** The E-Series Maintenance tab is not implemented in this release.

- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67. If you are already logged in, continue with [Step 2](#).
- Step 2** As needed, complete the following tasks:
- [DLP-A430 View Spanning Tree Information, page 21-9](#)
  - [DLP-A309 View the Ethernet MAC Address Table, page 20-4](#)
  - [DLP-A310 View Ethernet Trunk Utilization, page 20-5](#)
- Stop. You have completed this procedure.**

## NTP-A218 Change the Node Timing Reference

<b>Purpose</b>	This procedure enables automatic timing reference switching or returns the node timing to normal operation.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A28 Set Up Timing, page 4-9</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Maintenance or higher

- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67 at the node where you want to enable timing switching. If you are already logged in, continue with [Step 2](#).
- Step 2** Complete the “[DLP-A322 Manual or Force Switch the Node Timing Reference](#)” task on page 20-12 as needed.
- Step 3** Complete the “[DLP-A323 Clear a Manual or Force Switch on a Node Timing Reference](#)” task on page 20-13 as needed.
- Stop. You have completed this procedure.**

# NTP-A223 View the ONS 15454 Timing Report

<b>Purpose</b>	This procedure displays the current status of the ONS 15454 timing references.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A28 Set Up Timing, page 4-9</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- 
- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on [page 17-67](#) at the node where you want to view the node timing status. If you are already logged in, continue with [Step 2](#).
- Step 2** Click the **Maintenance > Timing > Report** tabs.
- Step 3** In the Timing Report area, you can view node timing information. The date and time of the report appear at the top of the report. The time stamp is the same as the alarms time stamp and can be configured using the “[DLP-A112 Display Alarms and Conditions Using Time Zone](#)” task on [page 18-2](#). [Table 15-2](#) on [page 15-18](#) describes the report fields and entries.
- Step 4** To update the report, click **Refresh**.

**Table 15-2 ONS 15454 Timing Report**

Item	Description	Option	Option Description
Clock	Indicates the timing clock. The report section that follows applies to the timing clock indicated.	NE	The node timing clock.
		BITS-1 Out	The BITS-1 Out timing clock.
		BITS-2 Out	The BITS-2 Out timing clock.

Table 15-2 ONS 15454 Timing Report (continued)

Item	Description	Option	Option Description
Status	Indicates the status of the timing clock.	INIT_STATE	The timing reference has not been provisioned. For an NE reference, this status appears just before the first provisioning messages when the TCC2/TCC2P is booting. Timing is provisioned to the internal clock of the node.
		HOLDOVER_STATE	The clock was locked onto a valid timing reference for more than 140 seconds when a failure occurred. Holdover state timing is a computation based on timing during normal state combined with the node's internal clock. The node holds onto this frequency until the valid reference is restored. This status appears for NE references only.
		FREERUN_STATE	The node is running off its internal clock without any modification except the calibrated value to bring timing to 0 PPM. Freerun state can occur when a Force switch to the Internal clock is initiated, all references fail without the 140 seconds of holdover data, or only Internal timing references are defined. This status appears for NE references only.
		NO_SYNC_STATE	A synchronization timing reference is not defined. BITS-1 Out or BITS-2 Out default to this status until an OC-N card is defined as its reference on the Provisioning > Timing tab. This status appears for external references only.
		NE_SYNCH_STATE	BITS-1 Out and BITS-2 Out use the same timing source as the NE. This is displayed when NE Reference is selected for BITS-1 Out and BITS-2 Out Reference List on the Provisioning > Timing tab.
		NORMAL_STATE	The timing reference is locked onto one of its provisioned references. The reference cannot be Internal or no sync state.
		FAST_START_STATE	The node has switched references, but the reference is too far away to reach normal state within an acceptable amount of time. Fast Start is a fast acquisition mode to allow the node to quickly acquire the reference. After it achieves this goal, the node progresses to the normal state.
Status (cont.)		FAST_START_FAILED_STATE	A timing reference is too far away to reach in normal state. The fast start state could not acquire sufficient timing information within the allowable amount of time.
Status Changed At	Date and time of the last status change.	—	—

Table 15-2 ONS 15454 Timing Report (continued)

Item	Description	Option	Option Description
Switch Type	Type of switch.	AUTOMATIC	The timing switch was system-generated.
		Manual	The timing switch was a user-initiated Manual switch.
		Force	The timing switch was user-initiated Force switch.
Reference	Indicates the timing reference.	Three timing references (Ref-1, Ref-2, and Ref-3) are available on the Provisioning > Timing tab.	These options indicate the timing references that the system uses, and the order in which they are called. (For example, if Ref-1 becomes available, Ref-2 is called.)
Selected	Indicates whether the reference is selected.	Selected references are indicated with an X.	—
Facility	Indicates the timing facility provisioned for the reference on the Provisioning > Timing tab.	BITS-1	The timing facility is a building integrated timing supply (BITS) clock attached to the node's BITS-1 pins.
		BITS-2	The timing facility is a BITS clock attached to the node's BITS-2 pins.
		OC-N card with port #	If the node is set to line timing, this is the OC-N card and port provisioned as the timing reference.
		Internal clock	The node is using its internal clock.
State	Indicates the timing reference state.	IS	The timing reference is in service.
		OOS	The timing reference is out of service.
Condition	Indicates the timing reference state.	OKAY	The reference is valid to use as a timing reference.
		OOB	Out of bounds; the reference is not valid and cannot be used as a timing reference, for example, a BITS clock is disconnected.
Condition Changed	Indicates the date and time of the last status change in MM/DD/YY HH:MM:SS format.	—	—
SSM	Indicates whether SSM is enabled for the timing reference.	Enabled	SSM is enabled.
		Disabled	SSM is not enabled.

Table 15-2 ONS 15454 Timing Report (continued)

Item	Description	Option	Option Description
SSM Quality	Indicates the SSM timing quality.	8 to 10 SSM quality messages might be displayed.	For a list of SSM message sets, see the <i>Cisco ONS 15454 Reference Manual</i> .
SSM Changed	Indicates the date and time of the last SSM status change in MM/DD/YY HH:MM:SS format.	—	—

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

## NTP-A287 Replace an In-Service Cross-Connect Card

<b>Purpose</b>	This procedure replaces an in service cross-connect card.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards, page 17-45</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	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

Removing any active card from the ONS 15454 can result in traffic interruption. Use caution when replacing cards and verify that only the standby card is being replaced.

- Step 1** Complete the [“DLP-A60 Log into CTC” task on page 17-67](#) at the node where you will replace the card.
- Step 2** From the View menu choose **Go to Network View**.
- Step 3** Click the **Alarms** tab, then complete the following substeps:
  - a. Verify that the alarm filter is not on. See the [“DLP-A227 Disable Alarm Filtering” task on page 19-17](#) as necessary.
  - b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.
- Step 4** Determine the active cross-connect card (XCVT/XC10G/XC-VXC-10G). The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is amber.




---

**Note** You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

---

- Step 5** If you want to replace the active cross-connect card, you must switch it to standby first by completing the following substeps. If you want to replace the standby card, skip this step and continue with [Step 6](#).
- a. In the node view, click the **Maintenance > Cross-Connect** tabs.
  - b. Under Cross Connect Cards, choose **Switch**.
  - c. Click **Yes** in the Confirm Switch dialog box.




---

**Note** After the active XCVT/XC10G/XC-VXC-10G goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

---

- Step 6** Physically remove the standby cross-connect card (XCVT/XC10G/XC-VXC-10G) from the ONS 15454.




---

**Note** An improper removal (IMPROPRMVL) alarm is raised when a card reseal is performed, unless the card is first deleted in CTC. The alarm clears after the card replacement is complete.

---

- Step 7** Insert the replacement cross-connect card (XCVT/XC10G/XC-VXC-10G) into the empty slot. The replacement card boots up and becomes ready for service after approximately one minute.

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

---

## NTP-A288 Replace the Fan-Tray Assembly

<b>Purpose</b>	This procedure replaces a malfunctioning fan-tray assembly.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



**Caution**

---

The 15454-FTA3 and 15454-FTA3-T fan-tray assemblies can only be installed in ONS 15454 R3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857-xx; 15454-SA-HD, P/N: 800-24848-xx). The fan-tray assembly includes a pin that prevents it from being installed in ONS 15454 shelf assemblies released before ONS 15454 R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3-T or 15454-FTA3 in an incompatible shelf assembly.

---



**Caution**

---

Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the backplane.

---

**Note**

The 15454-SA-ANSI or 15454-SA-HD shelf assembly and 15454-FTA-3 or 15454-FTA3 fan-tray assembly are required with the ONS 15454 XC-10G, OC-192, and OC-48 any slot (AS) cards.

**Note**

To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities.

**Step 1**

Review [Table 15-3](#) to ensure that you have compatible components when replacing the fan-tray assembly and note the alarms that will occur when an incompatibility occurs.

**Note**

If you need to determine the hardware that has been installed on a node, click the Inventory tab in node view.

**Table 15-3** *Incompatibility Alarms*

Shelf Assembly <sup>1</sup>	Fan Tray <sup>2</sup>	AIP <sup>3</sup>	10G Cards <sup>4</sup>	Ethernet Cards <sup>5</sup>	Alarms
—	—	No fuse	—	—	Mismatch of Equipment Attributes (MEA) on alarm interface panel (AIP)
NEBS3E or NEBS3	2A	2A	No	—	None
NEBS3E or NEBS3	2A	2A	Yes	—	MEA on 10G
NEBS3E or NEBS3	2A	5A	No	—	None
NEBS3E or NEBS3	2A	5A	Yes	—	MEA on 10G
ANSI or HD	2A	2A	No	—	None
ANSI or HD	2A	2A	Yes	2.5G compatible	MEA on fan tray, AIP, and Ethernet
ANSI or HD	2A	2A	Yes	10G compatible	MEA on fan tray and AIP
ANSI or HD	2A	5A	No	Either	None
ANSI or HD	2A	5A	Yes	2.5G compatible	MEA on fan tray and Ethernet
ANSI or HD	2A	5A	Yes	10G compatible	MEA on fan tray
ANSI or HD	5A	2A	No	Either	MEA on AIP
ANSI or HD	5A	2A	Yes	2.5G compatible	MEA on AIP and Ethernet
ANSI or HD	5A	2A	Yes	10G compatible	MEA on AIP
ANSI or HD	5A	5A	No	Either	None
ANSI or HD	5A	5A	Yes	Either	None

1. 15454-SA-NEBS3E (P/N: 800-07149-xx) or 15454-SA-NEBS3 (P/N: 800-06741-xx) = shelf assemblies released before ONS 15454 Release 3.1  
15454-SA-ANSI (P/N: 800-19857-xx) = ONS 15454 Release 3.1 and later shelf assembly  
15454-SA-HD (P/N: 800-24848-xx) = ONS 15454 Release 3.1 and later shelf assembly
2. 5A Fan Tray = 15454-FTA3 (P/N: 800-19858-xx) or 15454-FTA3-T (P/N: 800-21448-xx)  
2A Fan Tray = 15454-FTA2 (P/Ns: 800-07145-xx, 800-07385-xx, 800-19591-xx, 800-19590-xx)
3. 5A AIP (P/N: 73-7665-xx), 2A AIP (P/N: 73-5262-xx)
4. 10G cards include the XC-10G, OC-192, and OC-48 AS.
5. 2.5G indicates cards that are compatible with the XC and XCVT cross-connect cards: E100T-12, E1000-2, E100T-G, E1000-2-G, G1K-4, ML100T-12, ML1000-2. 10G indicates cards that are compatible with the XC10G cross-connect card: E100T-G, E1000-2-G, G1000-4, G1K-4, ML100T-12, ML1000-2.

**Step 2** Open the front door of the shelf assembly. If the shelf assembly does not have a front door, continue with [Step 4](#).

- a. Open the front door lock.

The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

- b. Press the door button to release the latch.
- c. Swing the door open.

**Step 3** Remove the front door (optional). If you do not want to remove the door, proceed to [Step 4](#).

- a. Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
- b. Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
- c. Secure the dangling end of the ground strap to the door or chassis with tape.

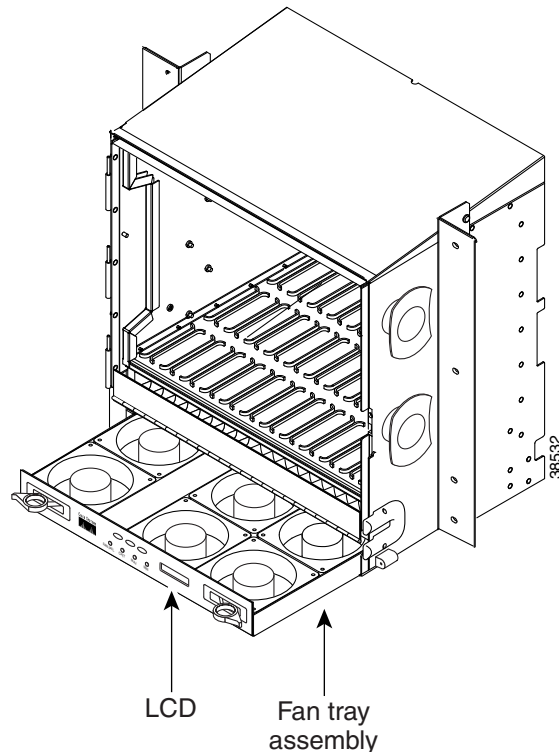
**Step 4** Push the outer side of the handles on the fan-tray assembly to expose the handles.

**Step 5** Fold out the retractable handles at the outside edges of the fan tray.

**Step 6** Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

**Step 7** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly. [Figure 15-5](#) shows the location of the fan tray.



**Figure 15-5** Removing or Replacing the Fan-Tray Assembly (Front Door Removed)

- Step 8** If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.
- If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the [“NTP-A107 Inspect, Clean, and Replace the Air Filter” procedure on page 15-2](#).
- Step 9** Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.
- Step 10** To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.
- Step 11** If you replace the door, be sure to reattach the ground strap.

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

---

# NTP-A290 Replace the Alarm Interface Panel

<b>Purpose</b>	This procedure replaces the alarm interface panel (AIP) with a new AIP on an in-service node without affecting traffic; however, shared packet rings might need to be deleted and rebuilt after the repair procedure. Ethernet circuits that traverse nodes with a software release prior to R4.0 will be affected.
<b>Tools/Equipment</b>	#2 Phillips screwdriver
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



## Warning

**The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed.**



## Caution

Do not use a 2A AIP with a 5A fan-tray assembly; doing so will cause a blown fuse on the AIP.



## Caution

If any nodes in an Ethernet circuit are not using Software R4.0 or later, there is a risk of Ethernet traffic disruptions. Contact the Cisco Technical Support at 1 800 553-2447 when prompted to do so in the procedure.



## Caution

Always use the supplied ESD wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.



## Caution

Do not perform this procedure on a node with live traffic. Hot-swapping the AIP can affect traffic and result in a loss of data. For assistance with AIP replacement contact Cisco Technical Support. See the [“Obtaining Documentation and Submitting a Service Request”](#) section on page Ixii.



## Note

Perform this procedure during a maintenance window. Resetting the active TCC2/TCC2P card can cause a service disruption of less than 50 ms to OC-N or DS-N traffic. Resetting the active TCC2/TCC2P card can cause a service disruption of 3 to 5 minutes on all Ethernet traffic due to spanning tree reconvergence if any nodes in the Ethernet circuit are not using Software R4.0 or later.

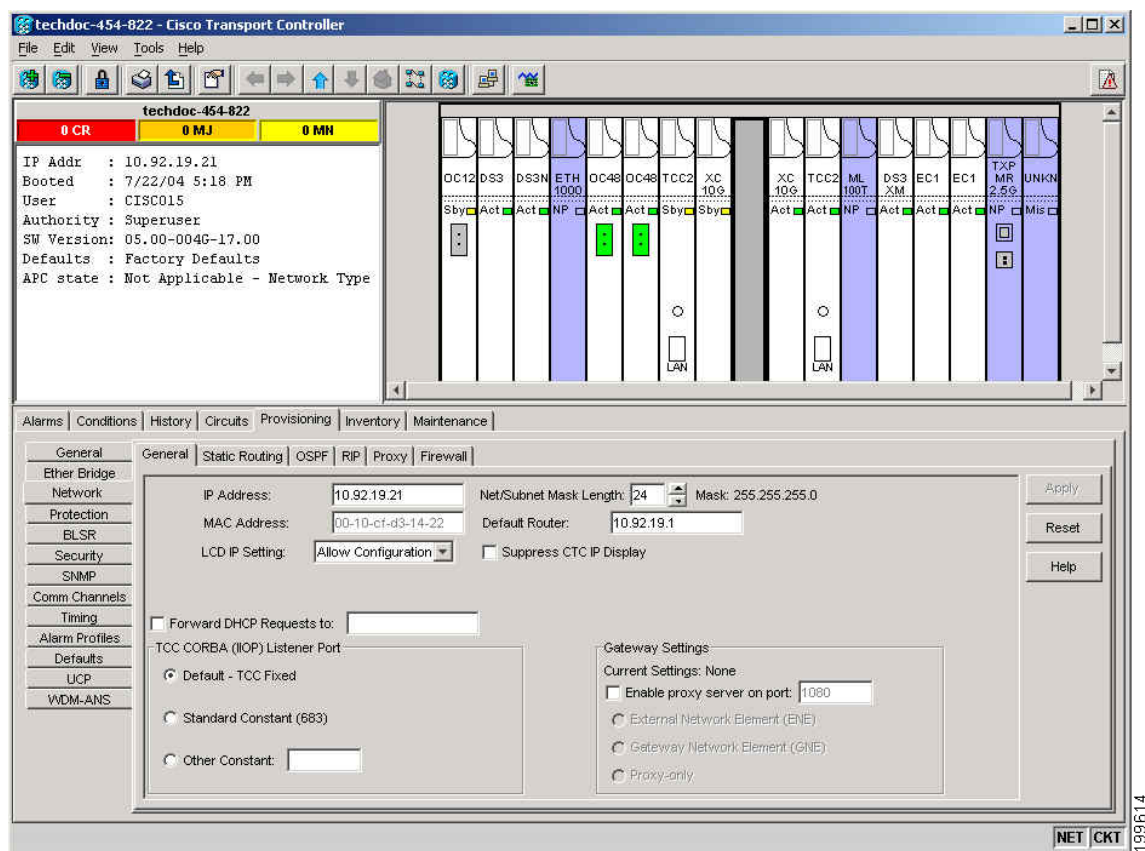
- Step 1** Review [Table 15-3 on page 15-23](#) to ensure that you have compatible components when replacing the fan-tray assembly and note the alarms that will occur when an incompatibility occurs.
- Step 2** Ensure that all nodes in the affected network are running the same software version by completing the following substeps before replacing the AIP and repairing circuits:
- Log into the node if you have not done so already by completing the [“DLP-A60 Log into CTC”](#) task on page 17-67.

- b. In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.
- c. If you need to upgrade the software on a node, refer to the release-specific software upgrade document for software upgrade procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to [Step 3](#).

**Step 3** Record the MAC address of the old AIP:

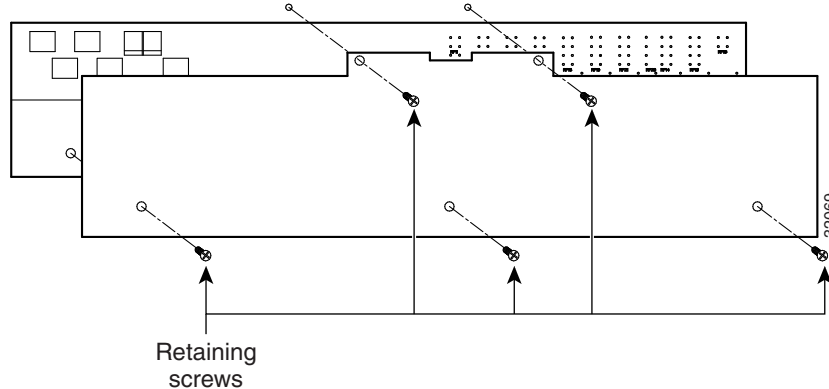
- a. If you are using a single IP address “repeater” configuration, click the **Provisioning > Network > General** tab.
- b. Record the MAC address shown in the General tab ([Figure 15-6](#)).

**Figure 15-6 Find the MAC Address in a Single IP Address Configuration**



(If you are using a secure dual IP mode configuration, the MAC addresses are shown in the **Provisioning > Security > Data Comm** tab.)

- Step 4** Call Cisco Technical Support for assistance in replacing the AIP and maintaining the original MAC address. See the [“Obtaining Documentation and Submitting a Service Request”](#) section on page Ixii.
- Step 5** Unscrew the five screws that hold the lower backplane cover in place ([Figure 15-7](#)).

**Figure 15-7 Lower Backplane Cover**

**Step 6** Grip the lower backplane cover and gently pull it straight away from the backplane.

**Step 7** Unscrew the two screws that hold the AIP cover in place.

**Step 8** Grip the cover and gently pull away from the backplane.



**Note** On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves, the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

**Step 9** Grip the AIP and gently pull it away from the backplane.

**Step 10** Disconnect the fan-tray assembly power cable from the AIP.

**Step 11** Set the old AIP aside for return to Cisco.

**Caution**

The type of shelf the AIP resides in determines the version of AIP that should replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) and 15454-SA-HD (P/N: 800-24848) currently use the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and earlier use the 2A AIP (P/N: 73-5262-01).

**Caution**

Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI shelf (P/N: 800-19857) or 15454-SA-HD (P/N: 800-24848); doing so will cause a blown fuse on the AIP.

**Step 12** Attach the fan-tray assembly power cable to the new AIP.

**Step 13** Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

**Step 14** Replace the AIP cover over the AIP and secure the cover with the two screws.

**Step 15** Replace the lower backplane cover and secure the cover with the five screws.

**Caution**

Cisco recommends that TCC2/TCC2P card resets be performed in a maintenance window to avoid any potential service disruptions.

- Step 16** Reset the standby TCC2/TCC2P card:
- Right-click the standby TCC2/TCC2P card and choose **Reset Card**.
  - Click **Yes** in the Resetting Card dialog box. As the card resets, a loading (Ldg) indication appears on the card in CTC.



---

**Note** The reset takes approximately five minutes. Do not perform any other steps until the reset is complete.

---

- Step 17** Complete the “[DLP-A364 Reset the TCC2/TCC2P Card Using CTC](#)” task on page 20-48 to reset the active TCC2/TCC2P card.
- Step 18** From the **File** menu, choose **Exit** to exit the CTC session.
- Step 19** Log back into the node. At the Login dialog box, choose (**None**) from the Additional Nodes drop-down list.
- Step 20** Record the new MAC address:
- In node view, click the **Provisioning > Network** tabs.
  - Record the MAC address shown in the General tab.



---

**Note** This location assumes a single IP, “repeater” configuration. For a secure, dual IP node, the IPs are viewable on the **Provisioning > Security > Data Comm** tab.

---

- Step 21** In node view, click the **Circuits** tab. Note that all circuits listed have a status of PARTIAL.
- Step 22** In node view, choose **Circuits > Repair Circuits** from the **Tools** menu. The Circuit Repair dialog box appears.
- Step 23** Read the instructions in the Circuit Repair dialog box ([Figure 15-8](#)). If all the steps in the dialog box have been completed, click **Next**. Ensure that you have the old and new MAC addresses.

**Figure 15-8**     **Repairing Circuits**



- Step 24** The Node MAC Addresses dialog box appears ([Figure 15-9](#)):
- From the Node drop-down list, choose the name of the node where you replaced the AIP.

- b. In the Old MAC Address field, enter the old MAC address that was recorded in [Step 3](#).
- c. Click **Next**.

**Figure 15-9** Recording the Old MAC Address Before Replacing the AIP



- Step 25** The Repair Circuits dialog box appears ([Figure 15-10](#)). Read the information in the dialog box and click **Finish**.

**Figure 15-10** Circuit Repair Information




---

**Note** The CTC session freezes until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned.

---

When the circuit repair is complete, the Circuits Repaired dialog box appears.

- Step 26** Click **OK**.
- Step 27** In the node view of the new node, click the **Circuits** tab. Check to ensure that all circuits listed have a status of DISCOVERED. If all circuits listed are not DISCOVERED, call the Cisco Technical Support to open a Return Material Authorization (RMA). See the [“Obtaining Documentation and Submitting a Service Request”](#) section on page lxii.

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

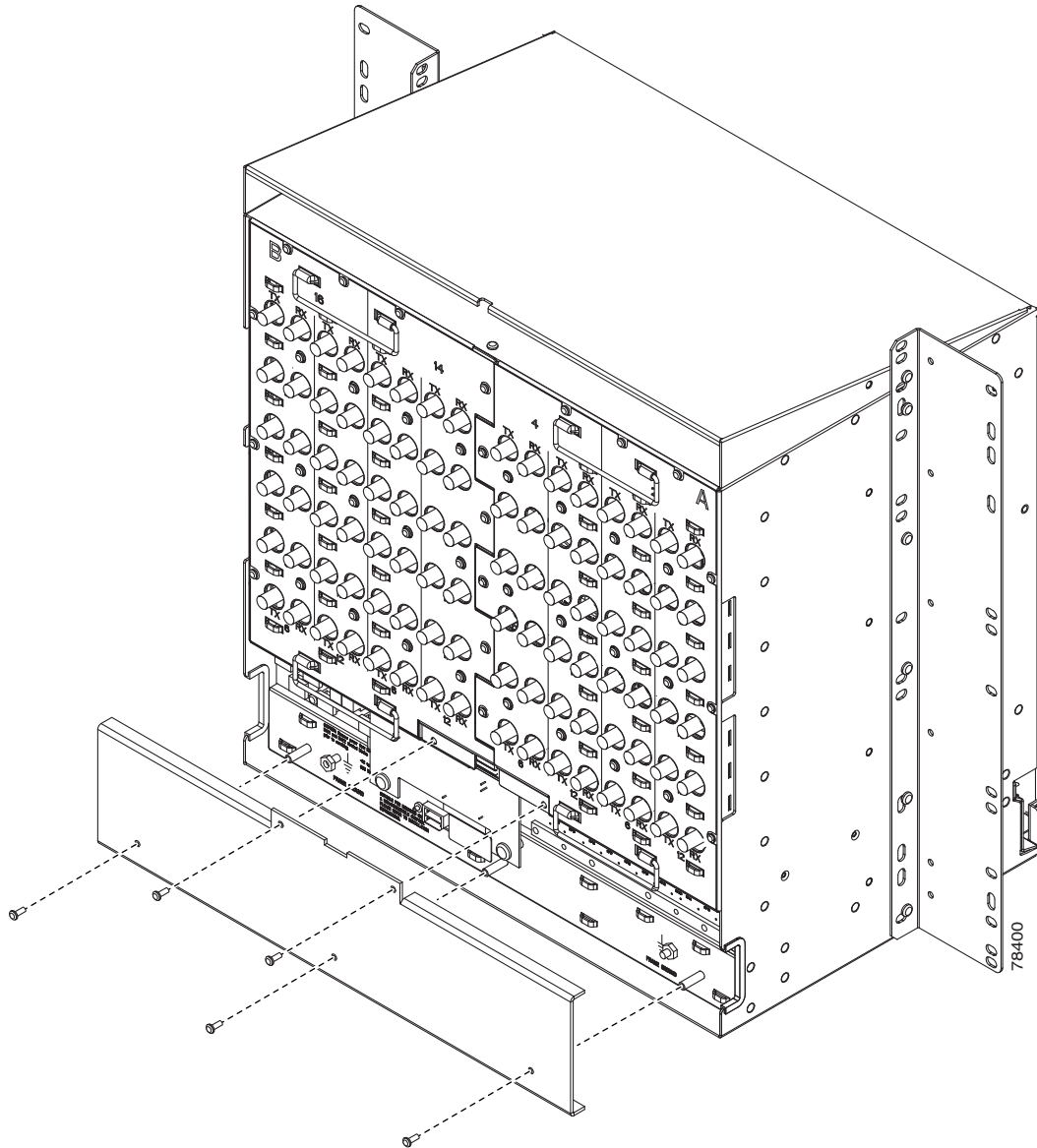
---

## NTP-A291 Replace the Plastic Lower Backplane Cover

<b>Purpose</b>	This procedure replaces the plastic cover located at the bottom rear of the ONS 15454.
<b>Tools/Equipment</b>	Phillips screwdriver
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

---

- Step 1** Use the Phillips screwdriver to unscrew the five retaining screws that hold the plastic cover in place.
- Step 2** Grasp the metal cover on each side.
- Step 3** Gently pull the plastic cover away from the backplane.
- Step 4** Place the plastic cover against the shelf assembly and align the screw holes on the cover and the shelf assembly ([Figure 15-11](#)).

**Figure 15-11** Attaching Plastic Lower Backplane Cover

- Step 5** Tighten the five retaining screws that hold the plastic cover in place.  
**Stop. You have completed this procedure.**
-

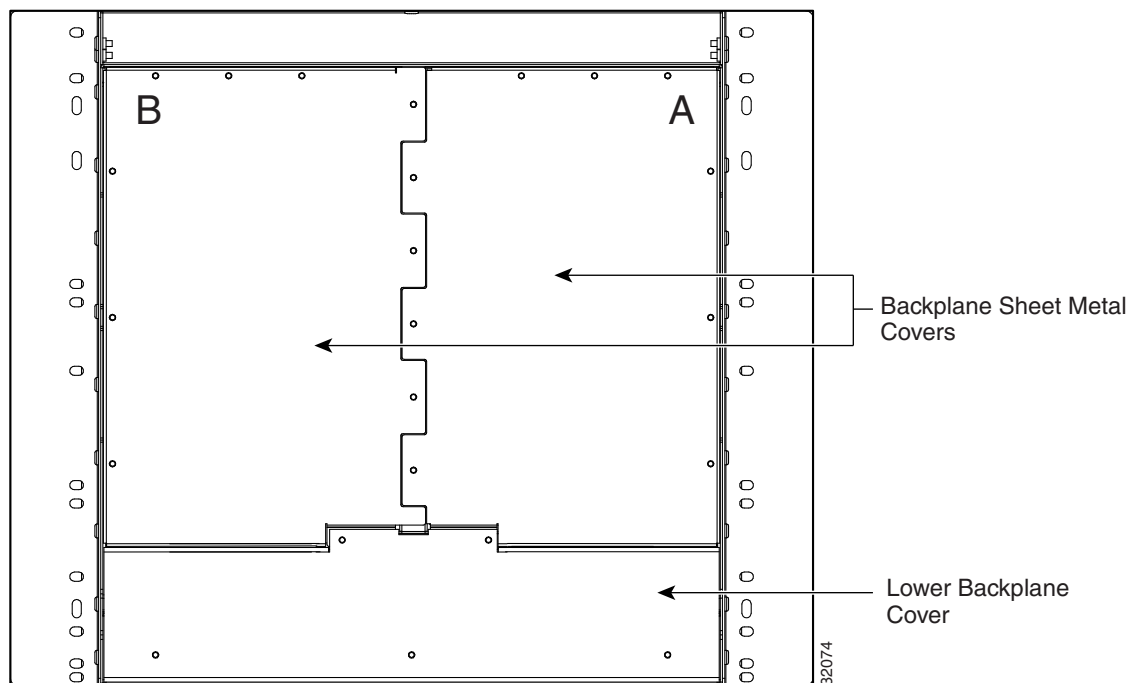


# NTP-A162 Replace the UBIC-V EIA

<b>Purpose</b>	This procedure replaces the UBIC-V EIA.
<b>Tools/Equipment</b>	#2 Phillips screwdriver Small slot-head screwdriver Replacement UBIC-V EIA and accompanying screws
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

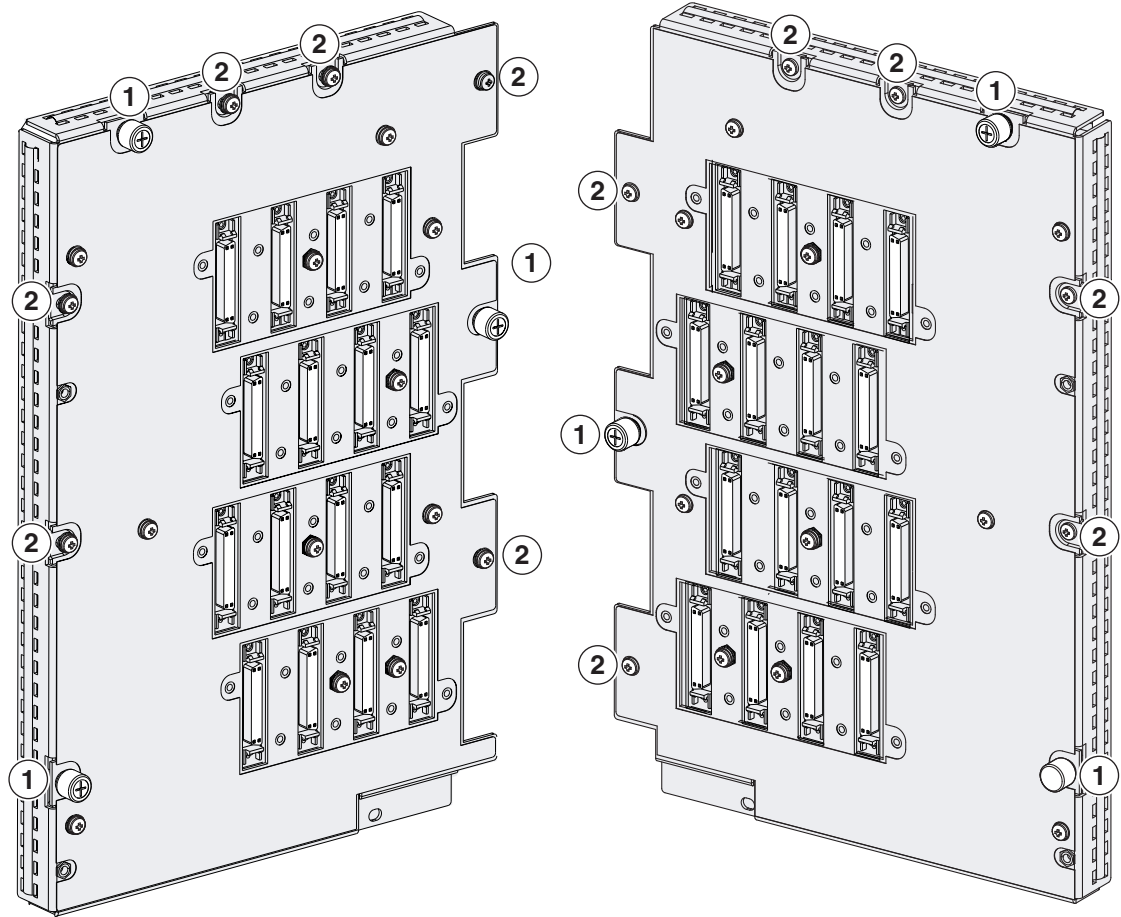
- Step 1** To remove the lower backplane cover, loosen and remove the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly (Figure 15-12).

**Figure 15-12** ONS 15454 Rear View (with Sheet Metal Covers Attached)



- Step 2** Loosen and remove the six perimeter screws that hold the sheet metal cover and UBIC-V in place (Figure 15-13).

Figure 15-13 UBIC-V EIA Screw Locations



- ① Jack screws (3)
- ② Perimeter screws, 6-32 x 0.375-inch Phillips head (6)

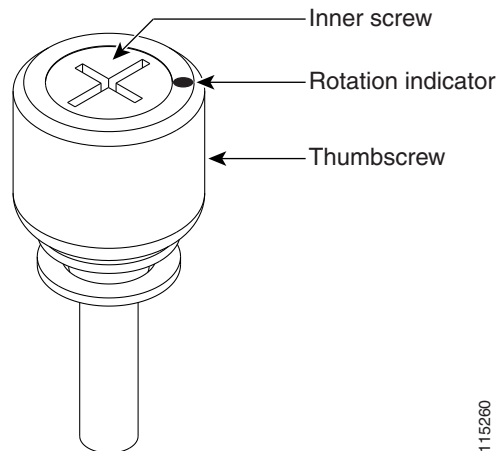
115140

**Step 3** Use a Phillips screwdriver to loosen each jack screw a maximum of two turns. Rotate each jack screw two turns at a time (per the rotation indicator) until all jack screws are fully disengaged (Figure 15-14).

**Caution**

Loosening the jack screws unevenly could cause damage to the UBIC-V connectors.

Figure 15-14 UBIC-V EIA Jack Screw



**Step 4** Grip two of the jack screws and use them to carefully pull the UBIC-V away from the shelf.



**Note** Attach backplane sheet metal covers whenever EIAs are not installed.

**Step 5** Perform the “[DLP-A190 Install a UBIC-V EIA](#)” task on page 18-56 to install the new UBIC-V EIA.  
**Stop. You have completed this procedure.**

## NTP-A336 Edit Network Element Defaults

<b>Purpose</b>	This procedure edits the NE defaults using the NE Defaults editor. The new defaults can either be applied only to the node on which they are edited or exported to a file and imported for use on other nodes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser



**Note** For a list of card and node default settings, refer to the “Network Element Defaults” appendix in the *Cisco ONS 15454 Reference Manual*. To change card settings individually (that is, without changing the defaults), see [Chapter 10, “Change Card Settings.”](#) To change node settings, see [Chapter 11, “Change Node Settings.”](#)

**Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67 at the node where you want to edit NE defaults.

**Step 2** Click the **Provisioning > Defaults** tabs.

- Step 3** Under Defaults Selector, choose a card type (if editing card-level defaults), **CTC** (if editing CTC 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 in the Default Name column. To selectively display just the defaults for a given card type, for node-level, or for CTC-level, you can drill down the Defaults Selector menu structure.
- Step 4** Locate a default you want to change under Default Name.
- Step 5** Click in the **Default Value** column for the default property you are changing and either choose a value from the drop-down menu (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 6** 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 7** If you are modifying node-level defaults, a dialog box appears telling you that applying defaults for node level attributes overrides current provisioning and asks if you want to continue. Click **Yes**.

If you are modifying the IOP 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 [Chapter 10, "Change Card Settings."](#)

---




---

**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-A337 Import Network Element Defaults

<b>Purpose</b>	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.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser



**Note** For a list of card and node default settings, refer to the “Network Element Defaults” appendix in the *Cisco ONS 15454 Reference Manual*.

- 
- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 17-67 at the node where you want to import NE defaults.
- Step 2** Click the **Provisioning > Defaults** tabs.
- Step 3** Click **Import**.
- Step 4** 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 you are importing.
- Step 5** When the correct file name and location appear in the dialog box (the correct file name is 15454-defaults.txt if you are importing the factory defaults), click **OK**.
- A pencil icon will appear next to any default value that will be changed as a result of importing the new defaults file.
- Step 6** Click **Apply**.
- Step 7** 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 8** If you are modifying node-level defaults, a dialog box appears telling you that applying defaults for node level attributes overrides current provisioning and asks if you want to continue. 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 [Chapter 10, “Change Card Settings.”](#)



**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-A338 Export Network Element Defaults

<b>Purpose</b>	This procedure exports the NE defaults using the NE Defaults Editor. The exported defaults can be imported to other nodes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser



**Note** The defaults currently displayed are exported whether or not they have been applied to the current node.



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

- Step 1** Complete the [“DLP-A60 Log into CTC” task on page 17-67](#) at the node where you want to export NE defaults.
- Step 2** Click the **Provisioning > Defaults** tabs.
- Step 3** Click **Export**.
- Step 4** If the desired file to export to does not appear in the Export Defaults to File dialog box (or does not yet exist) click **Browse** and browse to the directory where you want to export the data; then either choose or type in (to create) the file to export to [the defaults will be exported as a text file delimited by equals (=) signs].
- Step 5** Click **OK**.

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