
# Change Node Settings

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

This chapter explains how to modify node provisioning for the Cisco ONS 15327. To provision a new node, see Chapter 3, "Turn Up Node." To change default card-level and node-level settings, see Appendix C, "Network Element Defaults."

## Before You Begin

Before performing the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* as necessary.

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

1. NTP-B81 Change Node Management Information, page 9-2—As needed, complete this procedure to change node name, contact information, latitude, longitude, date, time, and the login legal disclaimer.
2. NTP-B201 Change CTC Network Access, page 9-4—As needed, complete this procedure to change the IP address, default router, subnet mask, network configuration settings, and static routes.
3. NTP-B202 Customize the CTC Network View, page 9-7—As needed, complete this procedure to customize the appearance of the network map, including specifying a different default map, selecting your own map or image, and changing the background color.
4. NTP-B203 Modify or Delete 1+1 Card Protection Settings, page 9-12—Complete as needed.
5. NTP-B85 Change Node Timing, page 9-15—Complete as needed.
6. NTP-B205 Modify Users and Change Security, page 9-17—Complete as needed.
7. NTP-B87 Change SNMP Settings, page 9-23—Complete as needed.

# NTP-B81 Change Node Management Information

| | |
|---|---|
| **Purpose** | This procedure changes basic information about the node such as node name, date, time, contact information, and the login legal disclaimer. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

**Step 2** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

**Step 3** Click the **Provisioning > General** tabs.

**Step 4** Complete the "DLP-B140 Change the Node Name, Date, Time, and Contact Information" task on page 9-2, as needed.

**Step 5** Complete the "DLP-B265 Change the Login Legal Disclaimer" task on page 9-3, as needed.

**Step 6** After confirming the changes, complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

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

# DLP-B140 Change the Node Name, Date, Time, and Contact Information

| | |
|---|---|
| **Purpose** | This procedure changes basic information such as node name, date, time, and contact information. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** Changing the date, time, or time zone may invalidate the node's performance monitoring counters.

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

**Step 2** Change any of the following:

- General: Node Name
- General: Contact
- Location: Latitude
- Location: Longitude

- Location: Description

**Note** To see changes to longitude or latitude on the network map, you must go to network view and right-click the specified node, then click **Reset Node Position**.

- Time: Use SNTP Server
- Time: Date (M/D/Y)
- Time: Time (H:M:S)
- Time: Time Zone
- Time: Use Daylight Saving Time

  See the "NTP-B25 Set Up Name, Date, Time, and Contact Information" procedure on page 3-5 for detailed field descriptions.

**Step 3** Click **Apply**. Confirm that the changes appear; if not, repeat the task.

**Step 4** Return to your originating procedure (NTP).

# DLP-B265 Change the Login Legal Disclaimer

| | |
|---|---|
| **Purpose** | Use this task to modify the legal disclaimer statement shown in the CTC login dialog box so that it will display customer-specific information when users log into the network. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Step 1** In node view, click the **Provisioning > Security > Legal Disclaimer > HTML** tabs.

**Step 2** The existing statement is a default, non-customer-specific disclaimer. If you want to edit this statement with specifics for your company, you can change the text. You can also use the following HTML commands to format the text:

-  Begins boldface font
-  Ends boldface font
-  Aligns type in the center of the window
-  Ends the center alignment
- <font=n, where n = point size> Changes the font to the new size
- </font> Ends the font size command
- <p> Creates a line break
- <sub> Begins subscript
- </sub> Ends subscript

- <sup> Begins superscript
- </sup> Ends superscript
- <u> Starts underline
- </u> Ends underline

**Step 3** If you want to preview your changed statement and formatting, click the **Preview** subtab.

**Step 4** Click **Apply**.

**Step 5** Return to your originating procedure (NTP).

# NTP-B201 Change CTC Network Access

| | |
|---|---|
| **Purpose** | This procedure changes essential network information, including IP settings, static routes, and OSPF options. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** Additional ONS 15327 networking information and procedures, including IP addressing examples, static route scenarios, Open Shortest Path First (OSPF) protocol, and routing information protocol options are provided in the IP Networking section of the *Cisco ONS 15327 Reference Manual*.

**Step 1** Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

**Step 2** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

**Step 3** Perform any of the following tasks as needed:

- DLP-B266 Change IP Settings, page 9-5
- DLP-B142 Modify a Static Route, page 9-6
- DLP-B143 Delete a Static Route, page 9-6
- DLP-B144 Disable the Open Shortest Path First Protocol, page 9-7
- DLP-B250 Set Up or Change Open Shortest Path First Protocol, page 3-10.

**Step 4** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

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

# DLP-B266 Change IP Settings

| | |
|---|---|
| **Purpose** | This task changes the IP address, subnet mask, default router, DHCP access, firewall access, and proxy server settings for the ONS 15327. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Step 1** In node view, click the **Provisioning > Network > General** tabs.

**Step 2** Change any of the following:

- IP Address
- Default Router
- Subnet Mask Length
- Forward DHCP Request To
- TCC CORBA (IIOP) Listener Port
- Gateway Settings

See the "NTP-B169 Set Up CTC Network Access" procedure on page 3-7 for detailed field descriptions.

**Step 3** Click **Apply**.

If you changed any of the network fields that will cause the node to reboot, the Change Network Configuration confirmation dialog box appears. If you changed a gateway setting, a confirmation appropriate to the gateway field appears. If you only changed the IP address fields, no confirmation dialog box appears.

**Step 4** If a confirmation dialog box appears, click **Yes**.

If you changed an IP address, subnet mask length, or TCC CORBA (IIOP) Listener Port, both XTC cards will reboot, one at a time. Confirm that the changes appear. If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15327 Troubleshooting Guide*, as needed.

**Step 5** Return to your originating procedure (NTP).

# DLP-B142 Modify a Static Route

| | |
|---|---|
| **Purpose** | Use this task to modify a static route on an ONS 15327. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In node view, click the **Provisioning** > **Network** tabs.

**Step 2** Click the **Static Routing** tab.

**Step 3** Click the static route you want to edit.

**Step 4** Click **Edit.**

**Step 5** In the Edit Selected Static Route dialog box, enter the following:

- Mask
- Next Hop
- Cost

See the "DLP-B65 Create a Static Route" task on page 3-9 for detailed field descriptions.

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

**Step 7** Return to your originating procedure (NTP).

# DLP-B143 Delete a Static Route

| | |
|---|---|
| **Purpose** | Use this task to delete an existing static route on an ONS 15327. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In node view, click the **Provisioning** > **Network** > **Static Routing** tabs.

**Step 2** Click the static route you want to delete.

**Step 3** Click **Delete**. A confirmation dialog box appears.

**Step 4** Click **Yes**.

**Step 5** Return to your originating procedure (NTP).

# DLP-B144 Disable the Open Shortest Path First Protocol

| | |
|---|---|
| **Purpose** | Use this task to disable the Open Shortest Path First (OSPF) routing protocol for an ONS 15327 LAN. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In node view, click the **Provisioning > Network > OSPF** tabs. The OSPF subtab has several options.

**Step 2** In the OSPF on LAN area, uncheck the **OSPF active on LAN** check box.

**Step 3** Click **Apply**. Confirm that the changes appear; if not, repeat the task.

**Step 4** Return to your originating procedure (NTP).

**Note** Disabling OSPF can cause an XTC reboot, which causes a temporary loss of connectivity to the node, but does not affect traffic.

# NTP-B202 Customize the CTC Network View

| | |
|---|---|
| **Purpose** | Use this procedure to modify the CTC network view, including grouping nodes into domains for a less-cluttered display, changing the network view background color, and using a custom image for the network view background. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | None |
| **Required/As needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

**Step 2** Complete the following tasks, as needed:

- DLP-B145 Change the Network View Background Color, page 9-8
- DLP-B267 Change the Default Network View Background Map, page 9-8
- DLP-B268 Apply a Custom Network View Background Map, page 9-9
- DLP-B148 Create Domain Icons, page 9-10
- DLP-B149 Manage Domain Icons, page 9-10

- DLP-B269 Enable Dialog Box Do-Not-Display Option, page 9-11

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

# DLP-B145 Change the Network View Background Color

| | |
|---|---|
| **Purpose** | This task changes the network view background color and the domain view background color (the area displayed when you open a domain). |
| **Tools/Equipment** | None |
| **Prerequisite procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

**Note** If you modify background colors, the change is stored in your CTC user profile on the local computer. The change does not affect other CTC users on different computers.

**Step 1** From the View menu choose **Go to Network View**.

**Step 2** Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

**Step 3** On the Choose Color dialog box, select a background color.

**Step 4** Click **OK**.

**Step 5** Return to your originating procedure (NTP).

# DLP-B267 Change the Default Network View Background Map

| | |
|---|---|
| **Purpose** | This task changes the default map of the CTC network view. |
| **Tools/Equipment** | None |
| **Prerequisite procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** If you modify the background image, the change is stored in your CTC user profile on the local computer. The change does not affect other CTC users on different computers.

**Step 1** From the View menu choose **Go to Network View**.

**Step 2** From the Edit menu, choose **Preferences**.

**Step 3** On the Preferences dialog box, click the **Map** tab, then check the **Use Default Map** check box if it is not already checked.

**Step 4** Click the **Default Maps** field and choose a default map from the pull-down menu. Map choices are: Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).

**Step 5** Click **Apply**. The new network map is displayed.

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

**Step 7** If the ONS 15327 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the ONS 15327 icons are visible.

**Step 8** If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

**Step 9** If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15327 icons are displayed at the magnification you want.

**Step 10** Return to your originating procedure (NTP).

# DLP-B268 Apply a Custom Network View Background Map

| | |
|---|---|
| **Purpose** | This task changes the background image or map on the CTC network view. |
| **Tools/Equipment** | None |
| **Prerequisite procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

**Note** You can replace the network view background image with any JPEG or GIF image that is accessible on a local or network drive. If you apply a custom background image, the change is stored in your CTC user profile on the local computer. The change does not affect other CTC users on different computers.

**Step 1** From the View menu choose **Go to Network View**.

**Step 2** Right-click the network or domain map and choose **Set Background Image**.

**Step 3** Click **Browse**. Navigate to the graphic file you want to use as a background.

**Step 4** Select the file. Click **Open**.

**Step 5** Click **Apply** and then click **OK**.

**Step 6** If the ONS 15327 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until all the ONS 15327 icons are visible.

**Step 7** If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

**Step 8** If you want to change the magnification of the icons, right-click the network view and choose **Zoom In** or **Zoom Out**. Repeat this step until the ONS 15327 icons are displayed at the magnification you want.

**Step 9** Return to your originating procedure (NTP).

# DLP-B148 Create Domain Icons

| | |
|---|---|
| **Purpose** | Use this task to create a domain icon to group ONS 15327 icons in CTC network view. |
| **Tools/Equipment** | None |
| **Prerequisite procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** All domain changes, such as added or removed nodes, are visible to all users who log into the network.

**Step 1** From the View menu choose **Go to Network View**.

**Step 2** Right-click the network map and choose **Create New Domain** from the shortcut menu.

**Step 3** When the domain icon appears on the map, click the map name and type the domain name.

**Step 4** Press **Enter**.

**Step 5** Return to your originating procedure (NTP).

# DLP-B149 Manage Domain Icons

| | |
|---|---|
| **Purpose** | Use this task to manage CTC network view domain icons. |
| **Tools/Equipment** | None |
| **Prerequisite procedures** | DLP-B60 Log into CTC, page 2-23<br>DLP-B148 Create Domain Icons, page 9-10 |
| **Required/As needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** All domain actions, such as adding or removing node icons, will be seen by all users who log into the network.

**Step 1** From the View menu choose **Go to Network View**.

**Step 2** Locate the domain action you want in Table 9-1 and complete the appropriate steps.

*Table 9-1 Managing Domains*

| Domain action | Steps |
|---|---|
| Move a domain | Drag and drop the node icon to the new location. |
| Rename a domain | Right-click the domain icon and choose **Rename Domain** from the shortcut menu. Type the new name in the domain name field. |
| Add a node to a domain | Drag and drop the domain icon to the domain icon. |
| Move a node from a domain to the network map | Open the domain and right-click a node. Select **Move Node Back to Parent View**. |
| Open a domain | • Double-click the domain icon.<br>• Right-click the domain and choose **Open Domain**. |
| Return to network view | Right-click the domain view area and choose **Go to Parent View** from the shortcut menu. |
| Preview domain contents | Right-click the domain icon and choose **Show Domain Overview**. The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, right-click the overview and select **Show Domain Overview**. |
| Remove domain | Right-click the domain icon and choose **Remove Domain**. Any nodes residing in the domain are returned to the network map. |

**Step 3** Return to your originating procedure (NTP).

# DLP-B269 Enable Dialog Box Do-Not-Display Option

| | |
|---|---|
| **Purpose** | Use this task to ensure that a user-selected “Do not display” dialog box preference is enabled for subsequent sessions or to disable the “Do not display” option. |
| **Tools/Equipment** | None |
| **Prerequisite procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** If any user who has rights to perform an operation (for example, creating a circuit) selects the “Do not show this dialog again” check box on a dialog box, the dialog box is not displayed for any other users who perform that operation on the network unless the command is overridden using the following task.

**Step 1** From the Edit menu, choose **Preferences**.

**Step 2** In the Preferences dialog box, click the **General** tab.

The Preferences Management area field lists all dialog boxes where "Do not show this dialog again" was checked.

**Step 3** Choose one of the following:

- **Don't Show Any**—Hides all do-not-display check boxes.
- **Show All**—Overrides do-not-display check box selections and displays all dialog boxes.

**Step 4** Click **OK**.

**Step 5** Return to your originating procedure (NTP).

# NTP-B203 Modify or Delete 1+1 Card Protection Settings

| | |
|---|---|
| **Purpose** | Use this procedure to modify or delete 1+1 card protection settings. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Caution** Modifying and deleting protection groups can be service affecting.

**Step 1** Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

**Step 2** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

**Step 3** Perform any of the following tasks as needed:

- DLP-B154 Modify a 1+1 Protection Group, page 9-13
- DLP-B155 Delete a Protection Group, page 9-14

**Step 4** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

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

# DLP-B154 Modify a 1+1 Protection Group

| | |
|---|---|
| **Purpose** | Use this task to modify a 1+1 protection group for any optical port (OC-3, OC-12, or OC-48). |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In node view, click the **Provisioning** > **Protection** tabs.

**Step 2** Under Protection Groups, click the 1+1 protection group you want to modify.

**Step 3** Under Selected Group, you can modify the following:

- Name—As needed, type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Bidirectional switching—As needed, check or uncheck
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion time menu. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time pull-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "NTP-B170 Create Optical Protection Groups" procedure on page 3-20 for field descriptions.

**Step 4** Click **Apply**. Confirm that the changes appear.

**Note** If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15327 Troubleshooting Guide*, as needed.

**Step 5** Return to your originating procedure (NTP).

## DLP-B155 Delete a Protection Group

| | |
|---|---|
| **Purpose** | Use this task to delete a 1+1 protection group. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In the node view, click the **Provisioning** > **Protection** tabs.

**Step 2** In the Protection Groups list, click the protection group you want to delete.

**Step 3** Click **Delete**.

**Step 4** Click **Yes** in the Delete Protection Group dialog box to confirm deletion. Confirm that the changes appear; if they do not, repeat Steps 1 through 3.

**Step 5** Return to your originating procedure (NTP).

# NTP-B204 Delete a SONET DCC Termination

| | |
|---|---|
| **Purpose** | Use this task to delete a SONET DCC termination on the ONS 15327. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B253 Provision SONET DCC Terminations, page 4-5 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** Deleting a DCC termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

**Step 1** Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

**Step 2** In node view, click the **Provisioning > SONET DCC** tabs.

**Step 3** Click the DCC termination you want to delete. Click **Delete**. The Delete SDCC Termination dialog box opens.

**Step 4** Select the **Set Port Out of Service** check box, as needed, if you want to change the OC-N port where the DCC terminated to out of service (this may be service affecting).

**Step 5** Click **Yes** to confirm. Confirm that the changes appear.

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

# NTP-B85 Change Node Timing

| | |
|---|---|
| **Purpose** | This procedure changes the SONET timing settings for the ONS 15327. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-B28 Set Up Timing, page 3-16 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

**Step 2** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

**Step 3** As needed, complete the "DLP-B157 Change the Node Timing Source" task on page 9-15.

**Step 4** If you need to change any internal timing settings, follow the "DLP-B70 Set Up Internal Timing" task on page 3-19 for the settings you need to modify.

**Caution** Internal timing is Stratum 3 and not intended for permanent use. All ONS 15327s should be timed to a Stratum 2 or better primary reference source.

**Step 5** If you need to verify timing after removing a node from a BLSR or a path protection, see the "DLP-B304 Verify BLSR Pass-Through Circuits" task on page 13-11.

**Step 6** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

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

# DLP-B157 Change the Node Timing Source

| | |
|---|---|
| **Purpose** | This task changes the SONET timing source for the ONS 15327 |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Caution** The following procedure may be service affecting and should be performed during a scheduled maintenance window.

**Step 1** In node view, click the **Provisioning > Timing** tabs.

**Step 2** In the General Timing section, change any of the following information:

- Timing Mode

**Note** Because mixed timing can cause timing loops, Cisco does not recommend using the Mixed Timing option. Use this mode with care.

- SSM Message Set
- Quality of RES
- Revertive
- Reversion Time

See the "DLP-B69 Set Up External or Line Timing" task on page 3-17 for field descriptions.

**Step 3** In the BITS Facilities section, you can change the following information:

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

- State
- Coding
- Framing
- Sync Messaging
- AIS Threshold
- LBO

**Step 4** Under Reference Lists, you can change the following information:

**Note** Reference lists define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's Mechanical Interface Cards. If you attach equipment to the MIC BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

- NE Reference
- BITS 1 Out/BITS 2 Out

**Step 5** Click **Apply**. Confirm that the changes appear.

**Note** If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15327 Troubleshooting Guide*, as needed.

**Step 6** Return to your originating procedure (NTP).

# NTP-B205 Modify Users and Change Security

| | |
|---|---|
| **Purpose** | Use this procedure to modify user and security properties for the ONS 15327. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-B30 Create Users and Assign Security, page 3-3 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Step 1** Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

**Step 2** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

**Step 3** Perform any of the following tasks as needed:

- DLP-B271 Change Node Security Policy - Single Node, page 9-17
- DLP-B272 Change Node Security Policy - Multiple Nodes, page 9-18
- DLP-B158 Change User and Security Settings - Single Node, page 9-19
- DLP-B160 Change User and Security Settings - Multiple Nodes, page 9-20
- DLP-B159 Delete User - Single Node, page 9-22
- DLP-B161 Delete User - Multiple Nodes, page 9-22

**Step 4** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

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

# DLP-B271 Change Node Security Policy - Single Node

| | |
|---|---|
| **Purpose** | This task changes the security policy for a single node, including idle user timeouts, user lockouts, password changes, and concurrent login policies. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

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

**Step 2** Under Idle User Timeout, you can modify the timeout times by clicking the hour (H) and minute (M) arrows. You can choose values between 0 and 16 hours, and 0 and 59 minutes.

**Step 3** Under User Lockout, you can modify the following:

- Failed Logins Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.

- Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

**Step 4** Under Concurrent Logins, click **Single Session Per User** if you want to limit users to a single login session.

**Step 5** Under Password Change, you can modify the following:

- Require [nn] different passwords...—Choose a value between 0 and 10 to determine how many different passwords have to be created before a password can be reused.
- ...or a waiting period of [nn] days before password reuse—Choose a value between 0 and 30 days to set the amount of time (in days) before a password can be reused.

Users can change their passwords after they meet one of the two conditions. For example, if you set the number of different passwords to 5 and the number of days to 20, users can reuse a password after they change the password 5 times or after 20 days elapse, whichever occurs first.

**Step 6** Click **Apply**. Confirm that the changes appear.

**Step 7** Return to your originating procedure (NTP).

# DLP-B272 Change Node Security Policy - Multiple Nodes

| | |
|---|---|
| **Purpose** | This task changes the security policy for multiple nodes, including idle user timeouts, user lockouts, password change, and concurrent login policies. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Step 1** From the View menu choose **Go to Network View**.

**Step 2** Click the **Provisioning > Security > Policy** tabs. A read-only table of nodes and their policies is displayed.

**Step 3** Click a node on the table that you want to modify, then click the **Change** button.

**Step 4** Under Idle User Timeout, you can modify the timeout times by clicking the hour (H) and minute (M) arrows. You can choose values between 0 and 16 hours, and 0 and 59 minutes.

**Step 5** Under User Lockout, you can modify the following:

- Failed Logins Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

**Step 6** Under Concurrent Logins, click **Single Session Per User** if you want to limit users to a single login session.

**Step 7** Under Password Change, you can modify the following:

- Require [nn] different passwords...—Choose a value between 0 and 10 to determine how many different passwords have to be created before a password can be reused.
- ...or a waiting period of [nn] days before password reuse—Choose a value between 0 and 30 days to set the amount of time (in days) before a password can be reused.

Users can change their passwords after they meet one of the two conditions. For example, if you set the number of different passwords to 5 and the number of days to 20, users can reuse a password after they change their password 5 times or after 20 days elapse, whichever occurs first.

**Step 8** Click **OK**.

**Step 9** On the Security Policy Change Results dialog box, confirm the changes, then click **OK**.

**Step 10** Return to your originating procedure (NTP).

# DLP-B158 Change User and Security Settings - Single Node

| | |
|---|---|
| **Purpose** | This task changes settings for an existing user at one node. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

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

**Step 2** Click the user whose settings you want to modify.

**Step 3** Click **Change**.

**Step 4** In the Change User dialog box, enter the following:

- New Password
- Confirm New Password
- Security Level
- You can also lock out the user by selecting the check box.

See the"NTP-B30 Create Users and Assign Security" procedure on page 3-3 for field descriptions.

**Step 5** Click **OK**.

**Note** User settings that you changed during this task will not appear until that user logs off and logs back in again.

**Step 6** Return to your originating procedure (NTP).

# DLP-B160 Change User and Security Settings - Multiple Nodes

| | |
|---|---|
| **Purpose** | This task changes settings for an existing user on multiple nodes. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Note** You must add the same user name and password to each node the user will access.

**Step 1** From the View menu, choose **Go to Network View**. Verify that all the nodes where you want to add users are accessible.

**Step 2** Click the **Provisioning > Security > Users** tabs. Highlight the user's name whose settings you want to change.

**Step 3** Click **Change**. The Change User dialog box appears.

**Step 4** In the Change User dialog box, enter the following:

- New Password
- Confirm New Password
- Security Level
- You can also lock out the user by selecting the check box.

See the "DLP-B75 Create a New User - Multiple Nodes" task on page 3-4 for field descriptions.

**Step 5** Click **OK**. A Change Results confirmation dialog box appears.

**Step 6** Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.

**Step 7** Return to your originating procedure (NTP).

# DLP-B315 Log Out a User - Single Node

| | |
|---|---|
| **Purpose** | Use this task to log out a user from a single node. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Step 1** In node view, click the **Provisioning > Security > Active Logins** tabs.

**Step 2** Choose the user you want to log out and click **Logout**.

**Step 3** On the Logout User dialog box, check **Lockout before Logout** if you want to prevent the user from logging in after logout. Parameters set under User Lockouts in the Policy tab determine when the user can log back in. Either a manual unlock by a Superuser is required or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-B271 Change Node Security Policy - Single Node" task on page 9-17 for more information.

**Step 4** Click **OK**.

**Step 5** Click **Yes** to confirm the logout.

**Step 6** Return to your originating procedure (NTP).

# DLP-B316 Log Out a User - Multiple Nodes

| | |
|---|---|
| **Purpose** | Use this task to log out a user from multiple nodes. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Step 1** From the view menu, chose **Go to Network View**.

**Step 2** Click the **Provisioning > Security > Active Logins** tabs.

**Step 3** Choose the user you want to log out.

**Step 4** Click **Logout**.

**Step 5** On the Logout User dialog box, check the nodes where you want to log out the user.

**Step 6** Check **Lockout before Logout** if you want to prevent the user from logging in after logout. Parameters set under User Lockouts in the Policy tab determine when the user can log back in. Either a manual unlock by a Superuser is required or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-B271 Change Node Security Policy - Single Node" task on page 9-17 for more information.

**Step 7** Click **OK**.

**Step 8** Click **Yes** to confirm the logout.

**Step 9** Return to your originating procedure (NTP).

# DLP-B159 Delete User - Single Node

| | |
|---|---|
| **Purpose** | Use this task to delete an existing user from a single node. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Note** CTC will allow you to delete other Superuser IDs if one Superuser ID remains. For example, you can delete the CISCO15 user if you have created another Superuser ID. Use this option with caution.

**Note** Users who are logged in when you delete them will not be logged out. The delete user action will take effect after the user logs out. To log out a user who is currently logged in, complete the "DLP-B315 Log Out a User - Single Node" task on page 9-20.

**Step 1** In node view, select the **Provisioning > Security > Users** tabs.

**Step 2** Choose the user you want to delete.

**Step 3** Click **Delete**.

**Step 4** In the Delete User dialog box, click **OK**. Confirm that the changes appear; if not, repeat the task.

**Step 5** Return to your originating procedure (NTP).

# DLP-B161 Delete User - Multiple Nodes

| | |
|---|---|
| **Purpose** | Use this task to delete an existing user from multiple nodes. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Note** CTC will allow you to delete other Superuser IDs if one Superuser ID remains. For example, you can delete the CISCO15 user if you have created another Superuser ID. Use this option with caution.

**Note** Users who are logged in when you delete them will not be logged out. The delete user action will take effect after the user logs out. To log out a user who is currently logged in, complete the "DLP-B316 Log Out a User - Multiple Nodes" task on page 9-21.

**Step 1** From the View menu choose **Go to Network View**.

**Step 2** Click the **Provisioning > Security > Users** tabs. Highlight the name of the user you want to delete.

**Step 3** In the Delete User dialog box, click **OK**. Confirm that the changes appear; if not, repeat the task.

**Step 4** Click **OK**. A User Deletion confirmation dialog box appears.

**Step 5** Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.

**Step 6** Return to your originating procedure (NTP).

# NTP-B87 Change SNMP Settings

| | |
|---|---|
| **Purpose** | Use this procedure to modify SNMP settings for the ONS 15327. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Step 1** Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

**Step 2** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

**Step 3** Perform any of the following tasks as needed:

- DLP-B273 Modify SNMP Trap Destination, page 9-24
- DLP-B163 Delete SNMP Trap Destinations, page 9-25
- DLP-B164 Delete Ethernet RMON Alarm Thresholds, page 9-25

**Step 4** Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

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

# DLP-B273 Modify SNMP Trap Destination

| | |
|---|---|
| **Purpose** | Use this task to modify the SNMP trap destinations on an ONS 15327 including community name, default UDP port, SNMP trap version, and maximum traps per second. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In node view, click the **Provisioning > SNMP** tabs.

**Step 2** Select a trap in the **Trap Destinations** dialog box.

For a description of SNMP traps, refer to the *Cisco ONS 15327 Reference Manual*.

**Step 3** Type the SNMP community name in the Community Name field.

**Note** The community name is a form of authentication and access control. The community name assigned to the ONS 15327 is case-sensitive and must match the community name of the NMS.

**Note** The default UDP port for SNMP is 162.

**Step 4** Set the Trap Version field for either SNMPv1 or SNMPv2.

Refer to your NMS documentation to determine which version to use.

**Step 5** Set your maximum traps per second in the Max Traps per Second field.

**Note** The value is the maximum number of traps per second that will be sent to the SNMP manager. If the field is set to 0, all traps are sent.

**Step 6** If you want to allow the ONS 15327 SNMP agent to accept SNMP SET requests on certain MIBs, select the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

**Step 7** Click **Apply**.

**Step 8** SNMP settings are now configured. To view SNMP information for each node, highlight the node IP address in the Trap Destinations area of the Trap Destinations screen. Confirm that the changes appear.

**Note** If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15327 Troubleshooting Guide*, as needed.

**Step 9** Return to your originating procedure (NTP).

# DLP-B163 Delete SNMP Trap Destinations

| | |
|---|---|
| **Purpose** | Use this task to delete SNMP trap destinations on an ONS 15327. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In node view, click the **Provisioning > SNMP** tabs.

**Step 2** Under Trap Destinations, click the trap you want to delete.

**Step 3** Click **Delete**. A confirmation dialog box appears.

**Step 4** Click **Yes**. Confirm that the changes appear; if not, repeat the task.

**Step 5** Return to your originating procedure (NTP).

# DLP-B164 Delete Ethernet RMON Alarm Thresholds

| | |
|---|---|
| **Purpose** | This task deletes remote monitoring (RMON) threshold crossing alarms for Ethernet ports. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-B60 Log into CTC, page 2-23 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In node view, click the **Provisioning > Ether Bridge > Thresholds** tabs.

**Step 2** Click the RMON alarm threshold you want to delete.

**Step 3** Click **Delete**. The Delete Threshold dialog box opens.

**Step 4** Click **Yes** to delete that threshold.

**Step 5** Return to your originating procedure (NTP).