Connect the PC and Log into the GUI for Cisco ONS 15454 DWDM and Cisco NCS 2000 Series

First Published: 2013-03-08

Last Modified: 2024-02-12

C H A P T E R 1

Connect the PC and Log into the GUI

This document explains how to connect Windows PCs and Solaris workstations to the Cisco ONS 15454 DWDM and Cisco NCS 2000 Series. This document also explains how to log into Cisco Transport Controller (CTC) software, which is the Operation, Administration, Maintenance and Provisioning (OAM&P) user interface. Procedures for connecting to the ONS 15454 ANSI, ONS 15454 ETSI or Cisco NCS 2000 Series using TL1 are provided in the Cisco NCS 2000 Series TL1 Command Guide.

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

The procedures and tasks described in this document for the Cisco ONS 15454 DWDM and Cisco NCS 2000 Series platform.

Note   Cisco ONS 15454 M2 chassis has reached its end-of-life status. For more information, see the Retirement Notification page.

Changes to This Document

The following table lists new and changed content made to this document since it was first published.

Table 1: Changes to This Document

Date	Change Summary
November 2011	Release 9.40—Added NTP-G323 Create or Delete a Perspective View, on page 58
March 2013	Revised the part number and included Release 9.6.0.3 features.
November 2016	Included Release 10.6.1 features.
June 2017	Added the Troubleshooting with RSA, on page 39 section.
March 2019	Added the DLP-G Log into CTC with Stored Login Credentials procedure.

Before You Begin

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

- NTP-G17 Set Up Computer for CTC, on page 3—Complete this procedure if your Windows PC or Solaris workstation has never been connected to an ONS 15454 and NCS 2000.

- NTP-G18 Set Up CTC Computer for Local Craft Connection to the Node, on page 11—Complete this procedure to set up your computer for an onsite craft connection to the ONS 15454 and NCS 2000.

- NTP-G19 Set Up a CTC Computer for a Corporate LAN Connection to the Node, on page 28—Complete this procedure to set up your computer to connect to the ONS 15454 and NCS 2000 using a corporate LAN.

- NTP-G21 Log into the GUI, on page 31—Complete this procedure to log into CTC.

- NTP-G190 Use the CTC Launcher Application to Manage Multiple ONS Nodes, on page 47—Complete this procedure to use the CTC launcher application.

Note Autonegotiation is enabled on the EMS, craft terminal, and TNC/TNCE/TSC/TSCE LAN ports by default. The Layer 2 switch (Cisco or third party equipment) ports where the LAN cables are connected, are also configured with the autonegotiation enabled.

For an ONS 15454 M6 shelf and NCS 2000, we recommend the use of RJ-45 port (craft terminal port or the EMS port) on the ECU and ECU2 to establish LAN connectivity. The advantages of using the RJ-45 ports on the ECU and ECU2 include:

- CAT-5 Ethernet cable connections can be managed better by routing the cable through the ECU and ECU2 ejector.

- If the TNC, TNCE, TSC, or TSCE card fails, the LAN connection is not lost during the TNC, TNCE, TSC, or TSCE card switch over.

If the ECU or ECU2 is absent, you can connect a CAT-5 Ethernet cable to the LAN port on the TNC/TNCE/TSC/TSCE card to create an external LAN connection.

NTP-G17 Set Up Computer for CTC

Purpose	This procedure configures your Windows PC or Solaris workstation to run CTC.
Tools/Equipment	Cisco ONS 15454 Release 9.3
Prerequisite Procedures	Install the Cisco ONS 15454, ONS 15454 M2,ONS 15454 M6, and NCS 2000 Shelf. Refer the Cisco ONS 15454 Hardware Installation Guide or Cisco NCS 2000 Series Hardware Installation Guide.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	None

Note   JRE 1.6 and 1.7 is required to log into nodes running Software Release 9.3 and later. Complete the DLP-G52 Change the JRE Version, on page 11 as needed.

Procedure

Step 1   If your computer does not have an appropriate browser installed, complete one of the following:

- To install Internet Explorer 6.x, 7.x, or 8.x on a Windows PC, download the browser from www.microsoft.com

- To install Mozilla 1.7 on a Solaris workstation, download the browser from www.mozilla.org

- To install Safari on a MacOS-X PC, download the browser from www.apple.com

     Note   Internet Explorer 8.x is supported on Windows 7, and Safari is supported on MacOS-X.

Step 2   (Windows PC only) Complete the DLP-G331 Adjust the Java Virtual Memory Heap Size (Windows), on page 32 to increase the size of the JVM heap to improve CTC performance.

Step 3   Complete one of the following:

- If your computer is a Windows PC, complete the DLP-G37 Run the CTC Installation Wizard for Windows PCs, on page 4.

- If your computer is a Solaris workstation, complete the DLP-G38 Run the CTC Installation Wizard for Solaris Workstations, on page 7.

Stop. You have completed this procedure.

DLP-G37 Run the CTC Installation Wizard for Windows PCs

Purpose	This task installs CTC online user manuals, Acrobat Reader 8.1.2, JRE 1.6, and CTC JAR files on Windows PCs.
Tools/Equipment	Cisco ONS 15454 DWDM or Cisco NCS 2000 Series software Setup.
Prerequisite Procedures	None
Required/As Needed	This task is required if you will use a Windows computer to run CTC and if any one of the following is true: - JRE 1.6 is not installed. - CTC online user manuals are not installed and are needed. - CTC JAR files are not installed and are needed.
Onsite/Remote	Onsite or remote
Security Level	None

Note   If you will log into nodes running CTC software earlier than Release 4.6, install JRE 1.3.1. To run CTC software R9.3, install JRE 1.6.

Procedure

Step 1   Verify that your computer has the following:

- Processor—Pentium III, 700 Mhz or faster

- RAM—384 MB recommended, 512 MB optimum

Note Processor and RAM requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM.

- Hard drive—20 GB hard drive recommended with at least 50 MB of space available

- Operating system—Windows 98 (1st and 2nd editions), Windows NT 4.0 (with Service Pack 6a), Windows 2000 (with Service Pack 3), Windows XP (with Service Pack 1), Windows Vista, or Windows 7. If your operating system is Windows NT 4.0, go to the next step. If your operating system is Windows Vista or Windows 7, go to Step 3, on page 5. For all others, go to Step 4, on page 5.

Step 2 Verify that Service Pack 6a or later is installed. From Windows Start menu, choose **Programs > Administrative Tools > Windows NT Diagnostics** and check the service pack on the Version tab of the Windows NT Diagnostics dialog box. If Service Pack 6a or later is not installed, do not continue. Install Service Pack 6a following the computer upgrade procedures for your site. Go to Step 4, on page 5.

Step 3 Complete DLP-G450 Configuring Windows Vista or Windows 7 to Support CTC, on page 57 and go to Step 4, on page 5

Step 4 Insert the Cisco ONS 15454 DWDM or Cisco NCS 2000 Series software CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to the CD directory and double-click **setup.exe**.

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- JRE 1.6

- Acrobat Reader 8.1.2

- Online User Manuals

- CTC JAR files

Note JRE 1.6 is required to run Release 9.3. Preinstalling the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TCC2/TCC2P/TCC3/TNC/TNCE/TSC/TSCE cards the first time you log in.

Step 5 Click **Next**.

Step 6 Complete one of the following:

- Click **Typical** to install the JRE, CTC JAR files, online user manuals, and Acrobat Reader. If you already have JRE 1.6 installed on your computer, choose **Custom**.

- Click **Custom** if you want to choose the components that you want to install. By default, Acrobat Reader and the online user manuals are selected.

Step 7 Click **Next**.

Step 8 Complete the following, as applicable:

- If you selected Typical in Step 6, on page 5 , skip this step and continue with Step 9, on page 6.

- If you selected Custom in Step 6, on page 5, check the CTC component that you want to install and click **Next**.

  - If you selected Online User Manuals, continue with Step 9, on page 6.

  - If you did not select Online User Manuals, continue with Step 11, on page 6.

Step 9 The directory where the installation wizard will install the CTC online user manuals appears. The default is C:\Program Files\Cisco\CTC\Documentation.

- If you want to change the CTC online user manuals directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.

- If you do not want to change the directory, continue with the next step.

Step 10 Click **Next**.

Step 11 Review the components that will be installed. If you want to change the components, complete one of the following. If not, proceed to the next step.

- If you selected Typical in Step 6, on page 5, click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Step 7, on page 5 through Step 10, on page 6.

- If you selected Custom in Step 6, on page 5, click **Back** once or twice (depending on the components selected) until the component selection page appears. Repeat Step 7, on page 5 through Step 10, on page 6.

Step 12 Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 6, on page 5 and you don't need to install a JRE, continue with Step 14, on page 7.

Step 13 To install the JRE, complete the following:

a) In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:

- I accept the terms of the license agreement—Accepts the license agreement. Continue with 13.b, on page 6.

- I do not accept the terms of the license agreement—Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 14, on page 7.

Note If JRE 1.6 is already installed on your computer, the Java 2 Runtime Environment License Agreement dialog box does not appear. You must click **Next** and then choose **Modify** to change the JRE installation, or **Remove** to uninstall the JRE. If you choose **Modify** and click **Next**, continue with Step 13.e, on page 6. If you choose **Remove** and click **Next**, continue with Step 13.i, on page 7.

b) Click Next.

c) Choose one of the following:

- Click Typical to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.

- Click Custom if you want to select the components to install and select the browsers that will use the JRE version.

d) Click Next.

e) If you selected Typical, continue with Step 13.i, on page 7. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 1.6 with support for European languages.

- Support for Additional Languages—Adds support for non-European languages.

- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

The drop-down list options for each program feature include:

- This feature will be installed on the local hard drive—Installs the selected feature.

- This feature and all subfeatures will be installed on the local hard drive—Installs the selected feature and all subfeatures.

- Don't install this feature now—Does not install the feature (not an option for Java 2 Runtime Environment).

  To modify the directory where the JRE version is installed, click Change, navigate to the desired directory, and click OK.

f) Click Next.

g) In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

   Note   Setting the JRE as the default for these browsers might cause problems with these browsers.

h) Click **Next**.

i) Click **Finish**.

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

Step 14   In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals and/or Adobe Acrobat Reader are installed.

Step 15   Click **Finish**.

Step 16   Return to your originating procedure (NTP).

DLP-G38 Run the CTC Installation Wizard for Solaris Workstations

Purpose	This task installs the CTC online user manuals, Acrobat 8.1.2, and JRE 1.6 on Solaris workstations, as necessary.
Tools/Equipment	Cisco ONS 15454 DWDM or Cisco NCS 2000 Series software Setup.
Prerequisite Procedures	None

Required/As Needed	This task is required if you will use a Solaris workstation to run CTC, and any of the following is true:
	• JRE 1.6 is not installed.
	• CTC online user manuals are not installed and are needed.
Onsite/Remote	Onsite or remote
Security Level	None

Note   If you will log into nodes running CTC software earlier than Release 4.6, install JRE 1.3.1. To run CTC software R9.3, install JRE 1.6.

Procedure

Step 1   Verify that your computer has the following:

- RAM—384 MB recommended, 512 MB optimum
- Hard drive—20 GB hard drive recommended with at least 50 MB of space available
- Operating system—Solaris 9 or 10

    Note   These requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM.

Step 2   Change the directory. Type:

cd /cdrom/cdrom0/

Step 3   From the techdoc454 CD directory, type:

./setup.bat

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- JRE 1.6
- Acrobat Reader 8.1.2
- Online User Manuals
- CTC JAR files

Step 4   Click **Next**.

Step 5   Complete one of the following:

- Click **Typical** to install the JRE, CTC JAR files, online user manuals, and Acrobat Reader. If you already have JRE 1.6 installed on your computer, choose **Custom**.

• Click **Custom** if you want to install either the JRE or the online user manuals.

Step 6   Click **Next**.

Step 7   Complete the following, as applicable:

- If you selected **Typical** in Step 5, on page 8 on page 10, continue with Step 8, on page 9 .

- If you selected **Custom** in xref, check the CTC component that you want to install and click **Next**.

    - If you selected Online User Manuals, continue with Step 8, on page 9.

    - If you did not select Online User Manuals, continue with DLP-G38 Run the CTC Installation Wizard for Solaris Workstations, on page 7 .

Step 8   The directory where the installation wizard will install the CTC online user manuals appears. The default is /usr/doc/ctc.

- If you want to change the CTC online user manuals directory, type the new directory path in the Directory Name field, or click Browse to navigate to the directory.

- If you do not want to change the CTC online user manuals directory, skip this step.

Step 9   Click **Next**.

Step 10   Review the components that will be installed.

- If you selected Typical in Step 5, on page 8 on page 10 , click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Step 6, on page 9 through Step 9, on page 9

- If you selected Custom in Step 5, on page 8 on page 10, click **Back** once or twice (depending on the components selected) until you reach the component selection page and check the desired components. Repeat Step 7, on page 9 on page 10 through Step 9, on page 9 on page 10.

Step 11   Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 7, on page 9 on page 10 and need to install the JRE, continue with Step 13, on page 10 on page 11

Step 12   To install the JRE, complete the following:

a) In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:

- I accept the terms of the license agreement—Accepts the license agreement. Continue with 12.b, on page 9 on page 11

- I do not accept the terms of the license agreement—Disables the **Next** button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 13, on page 10 on page 11

    Note   If JRE 1.6 is already installed on your computer, the Java 2 Runtime Environment License Agreement dialog box does not appear. You must click **Next** and then choose **Modify** to change the JRE installation or **Remove** to uninstall the JRE. If you choose **Modify** and click **Next**, continue with xref. If you choose **Remove** and click **Next**, continue with List item..

b) Click **Next.**

c) Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.

- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d) Click **Next.**

e) If you selected Typical, continue with on page 11. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 1.6 with support for European languages.

- Support for Additional Languages—Adds support for non-European languages.

- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

The drop-down list options for each program feature include:

- This feature will be installed on the local hard drive—Installs the selected feature.

- This feature and all subfeatures will be installed on the local hard drive—Installs the selected feature and all subfeatures.

- Don't install this feature now—Does not install the feature (not an option for Java 2 Runtime Environment).

To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK.**

f) Click **Next.**

g) In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

Note Setting the JRE as the default for these browsers might cause problems with these browsers.

h) Click **Next.**

i) Click **Finish**.

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

Step 13 In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals are installed.

Step 14 Click **Finish**.

Note Be sure to record the names of the directories you choose for JRE and the online user manuals.

Step 15 Return to your originating procedure (NTP).

DLP-G52 Change the JRE Version

Purpose	This task changes the JRE version, which is useful if you would like to upgrade to a later JRE version from an earlier one without using the software CD. This does not affect the browser default version. After selecting the desired JRE version, you must exit CTC. The next time you log into a node, the new JRE version will be used.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

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

Step 2   Click the **JRE** tab. The JRE tab shows the current JRE version and the recommended and supported versions.

Step 3   Click the **Browse** button and navigate to the JRE directory on your computer.

Step 4   Choose the JRE version.

Step 5   Click **Open**, then click **OK.**

Step 6   From the File menu, choose **Exit.**

Step 7   In the confirmation dialog box, click **Yes.**

Step 8   Log out of the ONS node.

Step 9   In the web browser that you used to log into the node, click **Delete CTC Cache**.

Step 10   Click **Yes** on the confirmation dialog then close the browser window.

Step 11   Complete the DLP-G46 Log into CTC.

Step 12   Return to your originating procedure (NTP).

NTP-G18 Set Up CTC Computer for Local Craft Connection to the Node

Purpose	This procedure explains how to set up a PC running Windows or a Solaris workstation for an onsite local craft connection to the node.

Tools/Equipment	Network interface card (NIC), also referred to as an Ethernet card Straight-through (CAT-5) LAN cable
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1 Complete one of the CTC computer setup tasks shown in the following table based on your CTC connection environment. For initial setup, use Option 1 or 3 if you are setting up a Windows PC. Use Option 4 if you are setting up a Solaris workstation.

Table 2: CTC Computer Setup for Local Craft Connections to the Node

Option	CTC Connection Environment	CTC Computer Setup Task
1	• You are connecting from a Windows PC. • You will connect to one ONS 15454, ONS 15454 M2, ONS 15454 M6 or NCS 2000. • You need to access non-ONS 15454 or non NCS 2000 applications such as ping and tracert (trace route).	DLP-G39 Set Up a Windows PC for Craft Connection on the Same Subnet Using Static IP Addresses, on page 15

Option	CTC Connection Environment	CTC Computer Setup Task
2	• You are connecting from a Windows PC. • Your network uses Dynamic Host Configuration Protocol (DHCP) for assignment of host IP addresses. • The CTC computer is provisioned for DHCP. • The ONS 15454 or NCS 2000 has DHCP forwarding enabled. • The ONS 15454 or NCS 2000 is connected to a DHCP server. **Note** The ONS 15454 or NCS 2000 does not provide IP addresses. If DHCP is enabled, it passes DCHP requests to an external DHCP server.	DLP-G40 Set Up a Windows PC for Craft Connection Using Dynamic Host Configuration Protocol, on page 18 **Note** Do not use this task for initial node turn-up. Use the task only if DHCP forwarding is enabled on the ONS 15454 or NCS 2000. By default, DHCP is not enabled. To enable it, refer the "NTP-G26 Set Up CTC Network Access" procedure", chapter "Turn up a Node" in the Cisco ONS 15454 DWDM Network Configuration Guide or Cisco NCS 2000 Series Network Configuration Guide.

Option	CTC Connection Environment	CTC Computer Setup Task
3	• You are connecting from a Windows PC. • You will connect to ONS 15454 or NCS 2000s at different locations and times and do not wish to reconfigure your PC's IP settings each time. • You will not access or use non-ONS 15454 or non-NCS 2000 applications such as ping and tracert (trace route). • If you are using an ANSI shelf, you will connect to the TCC2/TCC2P/TCC3 Ethernet port or backplane LAN pins either directly or through a hub. • If you are using an ETSI shelf, you will connect to the ONS 15454 or NCS 2000 Ethernet port or the RJ-45 jack on the MIC-C/T/P FMEC either directly or through a hub. • If you are using an ANSI or ETSI multishelf node, you will connect to the patch panel DCN port or the Catalyst 2950 or the Catalyst 3560 using a straight-through (CAT 5) LAN cable. • If you are using an ONS 15454 M6 or NCS 2000 shelf assembly, you will connect to the TNC/TNCE/TSC/TSCE ethernet port, or the EMS port or the craft terminal port on the ECU or ECU2 either directly or through a hub. • If you are using an ONS 15454 M2 or NCS 2000 shelf assembly, you will connect to the TNC/TNCE/TSC/TSCE ethernet port or the EMS port on the power module either directly or through a hub. • If you are using an ONS 15454 M6 or NCS 2000 multishelf node, you will connect to the patch panel DCN port or the Catalyst 2950 or Catalyst 3560 using a straight-through (CAT 5) LAN cable.	DLP-G41 Set Up a Windows PC for Craft Connection Using Automatic Host Detection, on page 22
4	• You are connecting from a Solaris workstation. • You will connect to one ONS 15454 or NCS 2000. • You need to access non-ONS 15454 or non-NCS 2000 applications such as ping and tracert (trace route).	DLP-G42 Set Up a Solaris Workstation for a Craft Connection, on page 26

Step 2 Connect a straight-through CAT-5 LAN cable from the Windows PC or Solaris workstation NIC to one of the following:

- The RJ-45 (LAN) port on the active or standby TCC2/TCC2P/TCC3 card. Use this method for the initial shelf turn-up.

- The RJ-45 (LAN) port on a hub or switch to which the ONS 15454 or NCS 2000 is physically connected.

- For multishelf mode, the DCN RJ-45 (LAN) port on the Ethernet Adapter Panel (EAP) or Port 23 or 24 of the Catalyst 2950 or the Catalyst 3560.

- If you are using an ONS 15454 M2 or NCS 2000 shelf assembly, you will connect to the TNC/TNCE/TSC/TSCE ethernet port or the EMS port on the power module either directly or through a hub.

- If you are using an ONS 15454 M6 or NCS 2000 shelf assembly, you will connect to the TNC/TNCE/TSC/TSCE ethernet port, or the EMS port or the craft terminal port on the ECU or ECU2 either directly or through a hub.

Note   For instructions on crimping your own straight-through (CAT-5) LAN cables, refer to the *Cisco ONS 15454 DWDM Troubleshooting Guide* or Cisco NCS 2000 Series Troubleshooting Guide.

Step 3   After setting up your CTC computer, continue with the NTP-G21 Log into the GUI, on page 31 as needed.

Stop. You have completed this procedure.

DLP-G39 Set Up a Windows PC for Craft Connection on the Same Subnet Using Static IP Addresses

Purpose	This task sets up your computer for a local craft connection to the ONS 15454 or NCS 2000 when:
	- You will connect to one ONS 15454 or NCS 2000; if you will connect to multiple ONS 15454 or NCS 2000, you might need to reconfigure your computer's IP settings each time you connect to an ONS 15454 or NCS 2000.
	- You need to use non-ONS 15454 or NCS 2000 applications such as ping and tracert (trace route).
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Procedure

Step 1   Verify the operating system that is installed on your computer:

a)   From the Windows Start menu, choose **Settings > Control Panel**.

b)   In the Control Panel window, double-click the **System** icon.

       c)   On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, Windows XP, Windows Vista, or Windows 7.

Step 2   According to the Windows operating system installed on your computer, perform one of the following steps:

     • For Windows 98, complete .

     • For Windows NT 4.0, complete .

     • For Windows 2000, complete .

     • For Windows XP, complete .

     • For Windows Vista, complete .

     • For Windows 7, complete .

Step 3   If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:

    a)   From the Windows Start menu, choose **Settings > Control Panel**.

    b)   In the Control Panel dialog box, click the **Network** icon.

    c)   In the Network dialog box, choose **TCP/IP** for your NIC card, then click **Properties.**

    d)   In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

    e)   Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

    f)   Click the **IP Address** tab.

    g)   In the IP Address window, click **Specify an IP address**.

    h)   In the IP Address field, enter an IP address that is identical to the ONS 15454 or NCS 2000 IP address except for the last octet. The last octet must be 1 or 3 through 254. This IP address appears on the LCD unless its display is suppressed during node provisioning.

    i)   In the Subnet Mask field, type the same subnet mask as the ONS 15454 or NCS 2000. The default is **255.255.255.0** (24 bit).

    j)   Click **OK.**

    k)   In the TCP/IP dialog box, click the **Gateway** tab.

    l)   In the New Gateway field, type the ONS 15454 or NCS 2000 IP address. Click **Add.**

    m) Verify that the IP address appears in the Installed Gateways field, then click **OK.**

    n)   When the prompt to restart your PC appears, click **Yes**.

    o)   Proceed to .

Step 4   If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

    a)   From the Windows Start menu, choose **Settings > Control Panel**.

    b)   In the Control Panel dialog box, click the **Network** icon.

    c)   In the Network dialog box, click the **Protocols** tab, choose **TCP/IP** Protocol, then click **Properties.**

    d)   Click the **IP Address** tab.

    e)   In the IP Address window, click **Specify an IP address**.

    f)   In the IP Address field, enter an IP address that is identical to the ONS 15454 or NCS 2000 IP address shown on the ONS 15454 or NCS 2000 LCD except for the last octet. The last octet must be 1 or 3 through 254.

    g)   In the Subnet Mask field, type**255.255.255.0.**

    h)   Click **Advanced.**

    i)   In the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box appears.

j) Type the ONS 15454 or NCS 2000 IP address in the Gateway Address field.

k) Click **Add.**

l) Click **OK.**

m) Click **Apply.**

n) In some cases, Windows NT 4.0 prompts you to reboot your PC. If you receive this prompt, click **Yes.**

o) Proceed to .

Step 5   If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

a) From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection**.

b) In the Local Area Connection Status dialog box, click **Properties.**

c) In the Network dialog box, click the **Protocols** tab, choose **TCP/IP** Protocol, then click **Properties.**

d) Click the **Use the following IP address** .

e) In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454 or NCS 2000. The default IP address is 192.1.0.2.

> **Note**   You can suppress the LCD IP address display using CTC. For more information, see the "DLP-G162 Change IP Settings" task on page 11-23.

f) In the Subnet Mask field, type the same subnet mask as the ONS 15454 or NCS 2000. The default is **255.255.255.0** (24 bit).

g) Type the IP address entered in Step e in the Gateway Address field.

h) Click **OK.**

i) In the Local Area Connection Properties dialog box, click **OK.**

j) In the Local Area Connection Status dialog box, click **Close.**

k) Proceed to .

Step 6   If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

a) From the Windows Start menu, choose **Control Panel > Network Connections**.

> **Note**   If the Network Connections menu is not available, right-click the Windows screen and choose **Properties** from the popup menu. Click the **Appearance** tab, then under Scheme, choose **Classic View**.

b) From the Network Connections dialog box, click the **Local Area Connection** icon.

c) On the General tab of the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties.**

d) In the IP Address field, enter an IP address that is identical to the ONS 15454 or NCS 2000 IP address shown on the ONS 15454 or NCS 2000 LCD except for the last octet. The last octet must be 1 or 3 through 254.

e) In the Subnet Mask field, type **255.255.255.0**.

f) In the Default Gateway field, type the ONS 15454 or NCS 2000 IP address.

g) Click **OK.**

h) In the Local Area Connection Properties dialog box, click **OK.**

i) In the Local Area Connection Status dialog box, click **Close.**

j) Proceed to .

Step 7   If you have Windows Vista installed on your PC, complete the following steps to change its TCP/IP configuration:

    a) From the Windows Start menu, choose **Control Panel > Network and Internet > Network and Sharing Center > Manage network connections**. The Manage network connections window appears.

    b) Right-click the **Local Area Connection** icon, then click **Properties**. The Local Area Connection Properties dialog box appears.

    c) Click the **Networking** tab. Under **This connection uses the following items**, click **Internet Protocol Version 4 (TCP/IPv4) > Properties**. The Networking dialog box appears.

    d) Click **Use the following IP address** and in the IP Address field, enter an IP address that is identical to the ONS 15454 or NCS 2000 IP address shown on the ONS 15454 or NCS 2000 LCD except for the last octet. The last octet must be 1 or 3 through 254.

    e) In the Subnet Mask field, type **255.255.255.0**.

    f) In the Default Gateway field, type the ONS 15454 or NCS 2000 IP address.

    g) Click **OK.**

    h) In the Local Area Connection Properties dialog box, click **OK.**

    i) Proceed to .

Step 8   If you have Windows 7 installed on your PC, complete the following steps to change its TCP/IP configuration:

    a) From the Windows Start menu, choose **Control Panel**.

    b) In the search box, type **adapter.**

    c) Under **Network and Sharing Center**, click **View Network Connections**. The Network Connections dialog box appears.

    d) In the Network Connections dialog box, right-click the **Local Area Connection** icon, then click **Properties**. The Local Area Connection Properties dialog box appears.

    e) Click the **Networking** tab. Under **This connection uses the following items**, click **Internet Protocol Version 4 (TCP/IPv4) > Properties**. The Networking dialog box appears.

    f) Click **Use the following IP address** and in the IP Address field, enter an IP address that is identical to the ONS 15454 or NCS 2000 IP address shown on the ONS 15454 or NCS 2000 LCD except for the last octet. The last octet must be 1 or 3 through 254.

    g) In the Subnet Mask field, type **255.255.255.0.**

    h) In the Default Gateway field, type the ONS 15454 or NCS 2000 IP address.

    i) Click **OK.**

    j) In the Local Area Connection Properties dialog box, click **OK.**

Step 9   Return to your originating procedure (NTP).

DLP-G40 Set Up a Windows PC for Craft Connection Using Dynamic Host Configuration Protocol

Purpose	This task sets up your computer for craft connection to the ONS 15454 or NCS 2000 using DHCP.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G17 Set Up Computer for CTC, on page 3 • NTP-G26 Set Up CTC Network Access

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

✎ **Note** Do not use this task for initial node turn-up. Use the task only if DHCP forwarding is enabled on the ONS 15454 or NCS 2000. By default, DHCP is not enabled. To enable it, see the chapter "Turn up a Node" in the *Cisco ONS 15454 DWDM Configuration Guide*.

✎ **Note** The ONS 15454 or NCS 2000 does not provide the IP addresses. If DHCP forwarding is enabled, it passes DCHP requests to an external DHCP server.

Procedure

Step 1 Verify the operating system that is installed on your computer:

    a) From the Windows Start menu, choose **Settings > Control Panel**.

    b) In the Control Panel window, double-click the **System** icon.

    c) On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, Windows XP, Windows Vista, or Windows 7.

Step 2 According to the Windows operating system installed on your computer, perform one of the following steps:

Step 3 If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:

    a) From the Windows Start menu, choose **Settings > Control Panel**.

    b) In the Control Panel dialog box, click the **Network** icon.

    c) In the Network dialog box, choose **TCP/IP** for your NIC card, then click **Properties.**

    d) In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

    e) Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

    f) Click the **IP Address** tab.

    g) In the IP Address window, click **Obtain an IP address automatically**.

    h) Click **OK.**

    i) When the prompt to restart your PC appears, click **Yes**.

       j)   Proceed to .

Step 4   If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

    a)   From the Windows Start menu, choose **Settings > Control Panel**.

    b)   In the Control Panel dialog box, click the **Network** icon.

    c)   In the Network dialog box, click the **Protocols** tab, choose **TCP/IP** Protocol, then click **Properties.**

    d)   Click the **IP Address** tab.

    e)   In the IP Address window, click **Obtain an IP address from a DHCP server**.

    f)   Click **OK.**

    g)   Click **Apply.**

    h)   If Windows prompts you to restart your PC, click **Yes.**

    i)   Proceed to .

Step 5   If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

    a)   From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection**.

    b)   In the Local Area Connection Status dialog box, choose the local area connection connected to the PC port connected to the ONS 15454 or NCS 2000.

    c)   In the Local Area Connection Status dialog box, click **Properties.**

    d)   On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

    e)   Click **Obtain an IP address automatically**.

    f)   Click **OK.**

    g)   In the Local Area Connection Properties dialog box, click **OK.**

    h)   In the Local Area Connection Status dialog box, click **Close.**

    i)   Proceed to .

Step 6   If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

    a)   From the Windows Start menu, choose **Control Panel > Network Connections**.

    Note   If the Network Connections menu is not available, right-click the Windows screen and choose **Properties** from the popup menu. Click the **Appearance** tab, then under Scheme, choose **Classic View**.

    b)   From the Network Connections dialog box, click the **Local Area Connection** icon.

    c)   On the General tab of the Local Area Connection Properties dialog box, click **Properties.**

    d)   On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties.**

    e)   Click **Obtain an IP address automatically**.

    f)   Click **OK.**

    g)   In the Local Area Connection Properties dialog box, click **OK.**

    h)   In the Local Area Connection Status dialog box, click **Close.**

    i)   Proceed to .

Step 7   If you have Windows Vista installed on your PC, complete the following steps to change its TCP/IP configuration:

    a)   From the Windows Start menu, choose **Control Panel > Network and Internet > Network and Sharing Center > Manage network connections**. The Manage network connections window appears.

    b)   Right-click the **Local Area Connection** icon, then click **Properties**. The Local Area Connection Properties dialog box appears.

    c) Click the **Networking** tab. Under **This connection uses the following items**, click **Internet Protocol Version 4 (TCP/IPv4) > Properties**. The Networking dialog box appears.

    d) Click **Obtain an IP address automatically.**

    e) Click **OK.**

    f) In the Local Area Connection Properties dialog box, click **OK.**

    g) Proceed to .

Step 8   If you have Windows 7 installed on your PC, complete the following steps to change its TCP/IP configuration:

    a) From the Windows Start menu, choose **Control Panel**.

    b) In the search box, type **adapter.**

    c) Under **Network and Sharing Center**, click **View Network Connections**. The Network Connections dialog box appears.

    d) Right-click the **Local Area Connection** icon, then click **Properties**. The Local Area Connection Properties dialog box appears.

    e) Click the **Networking** tab. Under **This connection uses the following items**, click **Internet Protocol Version 4 (TCP/IPv4) > Properties**. The Networking dialog box appears.

    f) Click **Obtain an IP address automatically.**

    g) Click **OK.**

    h) In the Local Area Connection Properties dialog box, click **OK.**

Step 9   Return to your originating procedure (NTP).

DLP-G41 Set Up a Windows PC for Craft Connection Using Automatic Host Detection

Purpose	This task sets up your computer for local craft connection to the ONS 15454 or NCS 2000 when: • You are using an ANSI shelf, you will connect to the ONS 15454 or NCS 2000 Ethernet port or backplane LAN pins either directly or through a hub. • You are using an ETSI shelf, you will connect to the ONS 15454 or NCS 2000 Ethernet port or the RJ-45 jack on the MIC-C/T/P FMEC either directly or through a hub. • You are using an ONS 15454 M6 shelf or NCS 2000 assembly, you will connect to the TNC/TNCE/TSC/TSCE ethernet port, or the EMS port or the craft terminal port on the ECU or ECU2 either directly or through a hub. • You are using an ONS 15454 M2 shelf or NCS 2000 assembly, you will connect to the TNC/TNCE/TSC/TSCE ethernet port or the EMS port on the power module either directly or through a hub. • You will connect to multiple ONS 15454 or NCS 2000 and do not want to reconfigure your IP address each time. • You do not need to access non-ONS 15454 or non-NCS 2000 applications such as ping and tracert (trace route).
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Procedure

Step 1   Verify the operating system that is installed on your computer:

     a)   From the Windows Start menu, choose **Settings > Control Panel**.

     b)   In the Control Panel window, double-click the **System** icon.

c) On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, Windows XP, Windows Vista, or Windows 7.

Step 2 According to the Windows operating system installed on your computer, perform one of the following steps:

- For Windows 98, complete .

- For Windows NT 4.0, complete .

- For Windows 2000, complete .

- For Windows XP, complete .

- For Windows Vista, complete .

- For Windows 7, complete .

Step 3 If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:

a) From the Windows Start menu, choose **Settings > Control Panel**.
b) In the Control Panel dialog box, click the **Network** icon.
c) In the Network dialog box, choose **TCP/IP** for your NIC card, then click **Properties.**
d) In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.
e) Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.
f) Click the **IP Address** tab.
g) In the IP Address window, click **Specify an IP address**.
h) In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454 or NCS 2000. The default IP address is 192.1.0.2.

Note You can suppress the LCD IP address display using CTC. For more information, see the "DLP-G162 Change IP Settings" task, chapter "Turn up a Node" in the *Cisco ONS 15454 DWDM Configuration Guide*.

i) In the Subnet Mask field, type the same subnet mask as the ONS 15454 or NCS 2000. The default is **255.255.255.0** (24 bit).
j) Click **OK.**
k) In the TCP/IP dialog box, click the **Gateway** tab.
l) In the New Gateway field, type the address entered in Step . Click **Add.**
m) Verify that the IP address appears in the Installed Gateways field, then click **OK.**
n) When the prompt to restart your PC appears, click **Yes**.
o) Proceed to .

Step 4 If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

a) From the Windows Start menu, choose **Settings > Control Panel**.
b) In the Control Panel dialog box, click the **Network** icon.
c) In the Network dialog box, click the **Protocols** tab, choose **TCP/IP** Protocol, then click **Properties.**
d) Click the **IP Address** tab.
e) In the IP Address window, click **Specify an IP address**.
f) In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454 or NCS 2000. The default IP address is 192.1.0.2.

Note	You can suppress the LCD IP address display using CTC. For more information, see the "DLP-G162 Change IP Settings" task, chapter "Turn up a Node" in the *Cisco ONS 15454 DWDM Configuration Guide*.

g) In the Subnet Mask field, type the same subnet mask as the ONS 15454 or NCS 2000. The default is **255.255.255.0** (24 bit).

h) Click **Advanced**.

i) In the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box appears.

j) Type the IP address entered in Step 4.f, on page 23 in the Gateway Address field.

k) Click **Add.**

l) Click **OK.**

m) Click **Apply.**

n) If Windows prompts you to restart your PC, click **Yes.**

o) Proceed to Step 9, on page 26.

Step 5 If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

a) From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection**.

b) In the Local Area Connection Status dialog box, click **Properties.**

c) On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d) Click **Use the following IP address.**

e) In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454 or NCS 2000. The default IP address is 192.1.0.2.

Note	You can suppress the LCD IP address display using CTC. For more information, see the "DLP-G162 Change IP Settings" task, chapter "Turn up a Node" in the *Cisco ONS 15454 DWDM Configuration Guide*.

f) In the Subnet Mask field, type the same subnet mask as the ONS 15454 or NCS 2000. The default is **255.255.255.0** (24 bit).

g) Type the IP address entered in Step 5.e, on page 24 in the Gateway Address field.

h) Click **OK.**

i) In the Local Area Connection Properties dialog box, click **OK.**

j) In the Local Area Connection Status dialog box, click **Close.**

k) Proceed to Step 9, on page 26.

Step 6 If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

a) From the Windows Start menu, choose **Control Panel > Network Connections**.

Note	If the Network Connections menu is not available, click **Switch to Classic View.**

b) From the Network Connections dialog box, click the **Local Area Connection** icon and select **Properties.**

c) On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties.**

d) In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454 or NCS 2000. The default IP address is 192.1.0.2.

e) Select the **Use the Following IP Address**: radio button.

Note	You can suppress the LCD IP address display using CTC. For more information, see the "DLP-G162 Change IP Settings" task, chapter "Turn up a Node" in the *Cisco ONS 15454 DWDM Configuration Guide*.

    f) In the Subnet Mask field, type the same subnet mask as the ONS 15454 or NCS 2000. The default is **255.255.255.0** (24 bit).

    g) Type the IP address entered in Step 6.d, on page 24 in the Gateway Address field.

    h) Click **OK.**

    i) In the Local Area Connection Properties dialog box, click **Close.**

    j) Proceed to Step 9, on page 26.

Step 7 If you have Windows Vista installed on your PC, complete the following steps to change its TCP/IP configuration:

    a) From the Windows Start menu, choose **Control Panel > Network and Internet > Network and Sharing Center > Manage network connections**. The Manage network connections window appears.

    b) Right-click the **Local Area Connection** icon, then click **Properties**. The Local Area Connection Properties dialog box appears.

    c) Click the **Networking** tab. Under **This connection uses the following items**, click **Internet Protocol Version 4 (TCP/IPv4) > Properties**. The Networking dialog box appears.

    d) Click **Use the following IP address** and in the IP Address field, enter any legitimate IP address other than the node IP address indicated on the LCD of the ONS 15454 or NCS 2000. The default IP address is 192.1.0.2.

Note	You can suppress the LCD IP address display using CTC. For more information, see the "DLP-G162 Change IP Settings" task, chapter "Turn up a Node" in the *Cisco ONS 15454 DWDM Configuration Guide*.

    e) In the Subnet Mask field, type the same subnet mask as the ONS 15454 or NCS 2000. The default is **255.255.255.0** (24 bit).

    f) Type the IP address entered in Step 7.d, on page 25 in the Gateway Address field.

    g) Click **OK.**

    h) In the Local Area Connection Properties dialog box, click **Close.**

    i) Proceed to Step 9, on page 26.

Step 8 If you have Windows 7 installed on your PC, complete the following steps to change its TCP/IP configuration:

    a) From the Windows Start menu, choose **Control Panel**.

    b) In the search box, type **adapter.**

    c) Under **Network and Sharing Center**, click **View Network Connections**. The Network Connections dialog box appears.

    d) Right-click the **Local Area Connection** icon, then click **Properties**. The Local Area Connection Properties dialog box appears.

    e) Click the **Networking** tab. Under **This connection uses the following items**, click **Internet Protocol Version 4 (TCP/IPv4) > Properties**. The Networking dialog box appears.

    f) Click **Use the following IP address** and in the IP Address field, enter any legitimate IP address other than the node IP address indicated on the LCD of the ONS 15454 or NCS 2000. The default IP address is 192.1.0.2.

Note	You can suppress the LCD IP address display using CTC. For more information, see the "DLP-G162 Change IP Settings" task, chapter "Turn up a Node" in the *Cisco ONS 15454 DWDM Configuration Guide*.

g) In the Subnet Mask field, type the same subnet mask as the ONS 15454 or NCS 2000. The default is **255.255.255.0** (24 bit).

h) Type the IP address entered in Step 8.f, on page 25 in the Gateway Address field.

i) Click **OK.**

j) In the Local Area Connection Properties dialog box, click **Close.**

Step 9   Return to your originating procedure (NTP).

DLP-G42 Set Up a Solaris Workstation for a Craft Connection

Purpose	This task sets up a Solaris workstation for a craft connection.
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

✎

Note   This procedure does not apply to the ONS 15454 M6, ONS 15454 M2 chassis, and NCS 2000 because they do not have a backplane TL1 craft port.

Procedure

Step 1   Log into the workstation as the root user.

Step 2   Check to see if the interface is plumbed by typing:

 # ifconfig *device*

For example:

 # ifconfig hme1

- If the interface is plumbed, a message similar to the following appears:

  hme1:flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 2 inet 0.0.0.0 netmask 0

  If a message similar to this one appears, go to Step 4, on page 27.

- If the interface is not plumbed, a message similar to the following appears:

  ifconfig: status: SIOCGLIFFLAGS: hme1: no such interface.

  If a message similar to this one appears, go to Step 3, on page 27.

Step 3 Plumb the interface by typing:

 # ifconfig *device* **plumb**

For example:

 # ifconfig hme1 plumb

Step 4 Configure the IP address on the interface by typing:

 # ifconfig *interface ip-address* **netmask** *netmask* **up**

For example:

 # ifconfig hme0 192.1.0.3 netmask 255.255.255.0 up

Note	Enter an IP address that is identical to the ONS 15454 or NCS 2000 IP address except for the last octet. The last octet must be 1 or 3 through 254.

Step 5 In the Subnet Mask field, type **255.255.255.0**. Skip this step if you checked Craft Access Only on the **Provisioning > Network > General > Gateway Settings** tab.

Step 6 Test the connection:

a) Start Mozilla.

b) Enter the ONS 15454 or NCS 2000 IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box appear. If this occurs, go to Step 2 of the DLP-G46 Log into CTC to complete the login. If the Login dialog box does not appear, complete Steps 6.c, on page 27 and 6.d, on page 27.

c) At the prompt, type:

ping *ONS-15454-IP-address*

For example, to connect to an ONS 15454 or NCS 2000 with a default IP address of 192.1.0.2, type:

ping 192.1.0.2

If your workstation is connected to the ONS 15454 or NCS 2000, the following message appears:

IP-*address* is alive

Note	Skip this step if you checked the Craft Access Only check box on the **Provisioning > Network > General > Gateway Settings** tab.

d) If CTC is not responding, a "no answer from x.x.x.x" message appears. Verify the IP and subnet mask information. Check that the cables connecting the workstation to the ONS 15454 or NCS 2000 are securely attached. Check the link status by typing:

 # ndd -set /dev/*device* **instance 0**

 # ndd -get /dev/*device* **link_status**

For example:

 # ndd -set /dev/hme instance 0

 # ndd -get /dev/hme link_status

A result of "1" means the link is up. A result of "0" means the link is down.

Note	Check the man page for ndd. For example, type: **# man ndd**.

Step 7   Return to your originating procedure (NTP).

NTP-G19 Set Up a CTC Computer for a Corporate LAN Connection to the Node

Purpose	This procedure sets up your computer to access the node through a corporate LAN.
Tools/Equipment	NIC, also referred to as an Ethernet card Straight-through (CAT-5) LAN cable
Prerequisite Procedures	• NTP-G17 Set Up Computer for CTC, on page 3 • The ONS 15454 or NCS 2000 must be provisioned for LAN connectivity, including IP address, subnet mask, default gateway. • The ONS 15454 or NCS 2000 must be physically connected to the corporate LAN.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1   If your computer is already connected to the corporate LAN, go to Step 3, on page 29. If you changed your computer's network settings for craft access to the ONS 15454 or NCS 2000, change the settings back to the corporate LAN access settings. This generally means:

- Set the IP Address on the TCP/IP dialog box back to **Obtain an IP address automatically** (Windows 2000 and XP) or **Obtain an IP address from a DHCP server** (Windows NT 4.0).

- If your LAN requires that Domain Name System (DNS) or Windows Internet Naming Service (WINS) be enabled, change the setting on the DNS Configuration or WINS Configuration tab of the TCP/IP dialog box.

Step 2   Connect the ONS 15454 or NCS 2000 and the computer to the corporate LAN:

- Connect a straight-through (CAT-5) LAN cable from the PC or Solaris workstation NIC card to a corporate LAN port.

- For a single ONS 15454 or NCS 2000 shelf node, connect a straight-through (CAT-5) LAN cable from the EMS or the craft terminal port to the corporate LAN port. For a single ONS 15454 M2 or NCS 2000

shelf, connect a straight-through (CAT-5) LAN cable from the EMS or the TNC/TNCE/TSC/TSCE Ethernet port to the corporate LAN port. For a single ONS 15454 M6 or NCS 2000 shelf, connect a straight-through (CAT-5) LAN cable from the EMS port, or the craft terminal port, or the TNC/TNCE/TSC/TSCE Ethernet port to the corporate LAN.

- For an ONS 15454 M6 or NCS 2000 multishelf node, connect a straight-through (CAT-5) LAN cable from the EMS port, or the craft terminal port, or the TNC/TNCE/TSC/TSCE Ethernet port. For an ONS 15454 or NCS 2000, connect the DCN RJ-45 (LAN) port on the EAP or to Port 23 or 24 of the Catalyst 2950 or the Catalyst 3560 to corporate LAN port.

Step 3 If your computer is connected to a proxy server, disable proxy service or add the ONS 15454 or NCS 2000 nodes as exceptions. To disable or bypass proxy service, complete one of the following tasks, depending on the web browser that you use:

Step 4 Continue with the .

Stop. You have completed this procedure.

DLP-G43 Disable or Bypass Proxy Service Using Internet Explorer (Windows)

Purpose	This task disables or bypasses proxy service for PCs running Internet Explorer.
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	Required if your computer is connected to a network computer proxy server and your browser is Internet Explorer.
Onsite/Remote	Onsite or remote
Security Level	None

Note If you disable proxy on a TCC2P/TCC3/TNC/TNCE/TSC/TSCE node that has secure mode enabled, the node's communication with other secure mode nodes may be compromised. For more information about secure mode, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 DWDM Network Configuration Guide* and *Cisco NCS 2000 Series Network Configuration Guide*.

Procedure

Step 1 From the Start menu, select **Settings > Control Panel**.

Note If your computer is running Windows XP, you can select Control Panel directly from the Start menu. Make sure that you are in Classic View before continuing with this procedure. To switch to Classic View, right-click the Windows screen and choose **Properties** from the popup menu. Click the **Appearance** tab, then under Scheme, choose **Classic View**.

Step 2 In the Control Panel window, choose **Internet Options**.

Step 3 In the Internet Properties dialog box, click **Connections > LAN Settings**.

Step 4 In the LAN Settings dialog box, complete one of the following tasks:

- Uncheck **Use a proxy server** to disable the service.

- To bypass the service, leave **Use a proxy server** selected and click **Advanced**. In the Proxy Setting dialog box under Exceptions, enter the IP addresses of ONS 15454 or NCS 2000 nodes that you will access. Separate each address with a semicolon. You can insert an asterisk (*) for the host number to include all the ONS 15454 or NCS 2000 on your network. Click **OK** to close each open dialog box.

Note For ONS 15454, ONS 15454 M2, ONS 15454 M6, and NCS 2000 nodes that have TCC2P/TCC3/TNC/TNCE/TSC/TSCE cards installed with the TCC2P/TCC3/TNC/TNCE/TSC/TSCE secure mode option enabled, enter the backplane LAN port (or the EMS port) IP addresses. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. For details about ONS 15454 nodes, see Management Network Connectivity. For details about NCS 2000 nodes, see Management Network Connectivity chapter in the Cisco ONS 15454 DWDM Reference Manual for more information about secure mode.

Step 5 Return to your originating procedure (NTP).

DLP-G44 Disable or Bypass Proxy Service Using Mozilla (Solaris)

Purpose	This task disables or bypasses proxy service for Windows PCs running Mozilla (Solaris). Required if your computer is connected to a network computer proxy server and your browser is Mozilla (Solaris).
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Note If you disable proxy on a TCC2P/TCC3/TNC/TNCE/TSC/TSCE node that has secure mode enabled, the node's communication with other secure mode nodes may be compromised. For more information about secure mode, see Management Network Connectivity.

Procedure

Step 1 Open Mozilla (Solaris).

Step 2 From the Edit menu, choose **Tools**. The Internet Options dialog box appears.

Step 3 In the Network tab, click **Settings**. The Connection Settings dialog box appears.

Step 4 In the Connection Settings dialog box, set one of the following options:

- Click the **No proxy** option to disable the proxy server.

- Click the **Auto-detect proxy settings for this network** option to automatically detect the proxy settings for the network.

- Click the **Manual proxy configuration** option to add exceptions to the proxy server. In the No Proxy For field, enter the IP addresses of the ONS 15454 or NCS 2000 nodes that you will access. Separate each address with a comma.

- Click **OK** to close the Connection Settings dialog box.

- Click **OK** to close the Internet Options dialog box.

| Note | For ONS 15454, ONS 15454 M2, ONS 15454 M6, or NCS 2000 nodes that have TCC2P, TCC3, TNC, TNCE, TSC, or TSCE cards installed with the TCC2P/TCC3/TNC/TNCE/TSC/TSCE secure mode option enabled, enter the backplane LAN port (or EMS port) IP addresses in the Manual proxy configuration option. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. |

Step 5 Return to your originating procedure (NTP).

NTP-G21 Log into the GUI

Purpose	This procedure logs into CTC, the graphical user interface (GUI) software used to manage the ONS 15454 or NCS 2000. This procedure includes optional node login tasks.
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3 One of the following procedures: • NTP-G18 Set Up CTC Computer for Local Craft Connection to the Node, on page 11 • NTP-G19 Set Up a CTC Computer for a Corporate LAN Connection to the Node, on page 28

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

Procedure

Step 1   Complete the DLP-G46 Log into CTC task.

> **Note**   For information about navigating in CTC, see CTC Enhancements, Operations, and Shortcuts

During network topology discovery, CTC polls each node in the network to determine which one contains the most recent version of the CTC software. If CTC discovers a node in the network that has a more recent version of the CTC software than the version you are currently running, CTC generates a message stating that a later version of the CTC has been found in the network. If you have network discovery disabled, CTC will not seek more recent versions of the software. Unreachable nodes are not included in the upgrade discovery.

> **Note**   Upgrading the CTC software will overwrite your existing software. You must restart CTC after the upgrade is complete.

Step 2   As needed, complete the DLP-G48 Create Login Node Groups, on page 41. Login node groups allow you to view and manage nodes that have an IP connection but no data communications channel (DCC) connection to the login node.

Step 3   As needed, complete the DLP-G49 Add a Node to the Current Session or Login Group, on page 42.

Step 4   As needed, complete the DLP-G50 Delete a Node from the Current Session or Login Group, on page 43.

Step 5   As needed, complete the DLP-G331 Adjust the Java Virtual Memory Heap Size (Windows), on page 32.

Step 6   As needed, complete the DLP-G51 Delete a Node from a Specific Login Node Group, on page 44.

Step 7   As needed, complete the DLP-G53 Configure the CTC Alerts Dialog Box for Automatic Popup, on page 45.

Stop. You have completed this procedure.

DLP-G331 Adjust the Java Virtual Memory Heap Size (Windows)

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

Note The task adjusts the physical memory allocation in the computer RAM so that more space is allocated for CTC. However, less physical memory will be available for other computer processes and programs. If you notice performance degradation of non-CTC programs after completing this task, reduce the JVM allotted to CTC. You may need to repeat the task a few times to find the right balance between JVM allotted to CTC and to other programs on your computer.

Procedure

Step 1 From the Windows PC, click **Start > Settings > Control Panel. > System**, or **Start > Control Panel > System** (Windows XP). The Windows Control Panel appears. The System Properties dialog box appears.

Step 2 Click the **Advanced** tab.

Step 3 Click **Environmental Variables**. The Environmental Variables dialog box appears.

Step 4 In the User Variables area, check to see whether a CTC_HEAP variable was created. If yes, complete the following steps. If not, continue with Step 5, on page 33.

 a) Check the CTC_HEAP value. If it is 512, continue with Step 12, on page 33. If not, continue with the next step.

 b) Click the CTC_HEAP variable and click **Edit**.

 c) In the Edit User Variable dialog box, enter the new JVM heap size. This can be any number between 256 and 512 MB.

 d) Click **OK**, then continue with Step 9, on page 33.

Step 5 Click **New**. The New User Variable dialog box appears.

Step 6 Type "CTC_HEAP" in the Variable Name field.

Step 7 Type "512" in the Variable Value field.

Step 8 Click **OK** to close the New User Variable dialog box.

Step 9 Click **OK** to close the Environmental Variables dialog box.

Step 10 Click **OK** to close the System Properties dialog box.

Step 11 Reboot your PC.

Step 12 Return to your originating procedure (NTP).

CTC Limitations

CTC might not start in systems running Windows 7 and Java 7. Perform the following steps to start CTC:

1. Remove all the Java versions from the system.

2. Reboot the system.

3. Install the appropriate JRE 1.7 from here.

4. Reboot the system again.

5. Start CTC.

From 9.6.0.3 release onwards, CTC is removed from Lite package. Hence, you cannot start CTC using a browser for a node having the TCC2P card as the controller card. The CTC standalone start application is required to start CTC. If startCTC.exe is not available, launch the CTC for the full package node having the TCC3/TNC/TSC/TNCE/TSCE card as the controller card, and add the Lite package node to the CTC.

DLP-G46 Log into CTC

Purpose	This task logs into the graphical user interface (GUI) of CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3 One of the following procedures: • NTP-G18 Set Up CTC Computer for Local Craft Connection to the Node, on page 11 • NTP-G19 Set Up a CTC Computer for a Corporate LAN Connection to the Node, on page 28
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

For information about CTC views and navigation, see "CTC Enhancements, Operations, and Shortcuts ."

(For 9.8.1, 10.0.1 releases and later) When the user attempts to log in to CTC, the node returns a new SSL Certificate. Hence, it is required to remove the existing node-related certificates stored in the browser to log in to CTC. When the user attempts to log in to CTC in EMS secure mode, the node displays a security warning message. Click **Continue** to ignore the warning message and log in to CTC.

CTC does not launch if the CTC cache directory has empty characters.

Procedure

Step 1   (For 9.8.1, 10.0.1 releases and later) Remove the existing node-related certificates from the web browser:

a)   Internet Explorer: Go to **Tools** -> **Internet Options** -> **Content** -> **Certificates** button.

b)   Mozilla Firefox: Go to **Options** -> **Advanced** -> **Certificates** -> **View Certificates** button.

c)   Check the certificates stored in all the tabs.

d)   If the certificate entries have the node IP address, servercard, or localhost, click **Delete** in Mozilla Firefox or click **Remove** in Internet Explorer to remove the certificates.

e)   Close the web browser.

Step 2   From the computer connected to the ONS 15454 or NCS 2000, start the web browser:

• If you are using a Windows PC, launch Internet Explorer or Mozilla from the Windows Start menu or a shortcut icon.

• If you are using a Solaris workstation, navigate to the directory where Mozilla was installed, then type:

 # mozilla -install

Step 3   In Internet Explorer or Mozilla web address (URL) field, enter the ONS 15454 or NCS 2000 IPv4 or IPv6 address. For initial setup, this is the default IP address, 192.1.0.2.

| **Note** | The IP address appears on the LCD. You can suppress the LCD IP address display using CTC after you log in. For more information, see the "DLP-G162 Change IP Settings" task, chapter "Turning Up a Node" in the *Cisco ONS 15454 DWDM Configuration Guide* and *Cisco NCS 2000 Series Network Configuration Guide*. |

Step 4   Press **Enter**. The CTC Launcher window is displayed. The CTC Launcher window has the following fields:

• Connection Mode area:

• Use IP—Enter the ONS NE node name or IP address. IP address of the node entered in the browser address field is pre-populated.

| **Note** | To log into CTC using an IPv6 address, you must first log into CTC using an IPv4 address and assign an IPv6 address to the node. Then, use the IPv6 address that you assigned to the node to log into CTC. For more information about configuring IPv6 address, see the "DLP-G162 Change IP Settings" task, chapter "Turn up a Node" in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. Enter the IPv6 address in the address bar of the browser, enclosed in square brackets. |

• Use TL1 Tunnel—Choose this option to connect to the node through a TL1 tunnel. See the sedstion "Setting Up TL1 Communication" in the "Procedures and Provisioning" chapter of the *Cisco ONS SDH TL1 Reference Guide* or the *Cisco ONS SONET TL1 Reference Guide*.

• CTC Version Selection—Software version to launch CTC. Select from the following choices in the drop-down menu:

• Same version as the login node—Select if you want to launch the same CTC version as the login node version, even if more recent versions of CTC are available in the cache.

• Latest version available—Select if you want to launch the latest CTC version available. If the cache has a newer CTC version than the login node, that CTC version will be used. Otherwise the same CTC version as the login node will be used.

• Version x.xx—Select if you want to launch a specific CTC version.

| **Note** | If you are logging into ONS 15454 or NCS 2000 nodes in an operation network that are running different releases of CTC software, log into the node running the most recent release. If you log into a node running an older release, you will receive an INCOMPATIBLE-SW alarm for each node in the network running a new release, and CTC will not be able to manage these nodes. To check the software version of a node, select About CTC from the CTC Help menu. This will display the ONS 15454 or NCS 2000 software version for each node visible on the network view. If the node is not visible, the software version can be read from the LCD display. To resolve an alarm, refer to the Cisco ONS 15454 DWDM Troubleshooting Guide and Cisco NCS 2000 Series Troubleshooting Guide. |

• Settings—Displays the CTC Launcher Settings window with the following fields:

• Cache tab

> • Cache Directory List—Lists the cache directories.
>
> • Add—Provides an option to add a cache directory.
>
> • Delete—Deletes a cache directory. The default CTC cache directory cannot be deleted.
>
> • Move Up—Moves up a selected CTC cache directory.
>
> • Move Down—Moves down a selected CTC cache directory.
>
> • Delete Cache—Deletes the CTC JAR (Java Archive) files that are downloaded to your computer when you log into a CTC node. You perform this action if connectivity problems occur or you want to delete older CTC JAR file versions from your computer. For more information, refer to the "General Troubleshooting" chapter in the Cisco ONS 15454 DWDM Troubleshooting Guide and Cisco NCS 2000 Series Troubleshooting Guide.

• JVM tab

> • Maximum Java Heap Size (MB)—Provides option to specify maximum Java heap size.
>
> **Note** The Java heap size must be less than the total system physical memory.
>
> • Maximum Java Perm Size (MB)—Provides option to specify maximum Java PermSize.

• OK—Saves any changes and closes the CTC Launcher Settings window.

• Cancel—Cancels any changes and closes the CTC Launcher Settings window.

• Apply—Saves any changes but does not close the CTC Launcher Settings window.

• Launch CTC—After the connection is made, the CTC Login dialog box appears.

If a Java Plug-in Security Warning dialog box appears, complete the DLP-G47 Install Public-Key Security Certificate, on page 40 task to install the public-key security certificate required by Software Release 4.1 and later.

After you complete the security certificate dialog box (or if the certificate is already installed), a Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to an ONS 15454 or NCS 2000, this process can take several minutes. After the download, a warning message window appears.

• Cancel—Cancels the CTC connection and closes the CTC Launcher window.

Step 5 In the Login dialog box, perform the following steps:

a) For initial setup, type the user name **CISCO15** and the password **otbu+1**

Note The user name and password are case sensitive. The CISCO15 user is provided with every ONS 15454 or NCS 2000. CISCO15 has Superuser privileges, so you can create other users. You must create another Superuser before you can delete the CISCO15 user. CISCO15 is delivered with the otbu+1 password. To change the password for CISCO15, complete the "DLP-G191 Change User Password and Security Level on a Single Node" task in Manage the Node document after you login.

b) See the DLP-G Log into CTC with Stored Login Credentials to log into CTC with stored login credentials.

c) For other logins, type a user name in the **User Name** field.

d) If you are logging in for the first time, generate a new Tokencode using the **RSA SecureID**. When you are logging in for the second time or the subsequent logins, enter the saved PIN in the **RSA SecureID** and generate a new Passcode.

e) Enter the Tokencode or Passcode in the **Password** field and click **Login**.

f) Enter **Y** in the **Challenge/Response** window to generate a new PIN and click **OK**.

If you enter anything other than **Y**, PIN will not be generated and the authentication will fail.

g) Type the PIN in the **Challenge/Response** window and click **OK**.

Note	If the CTC session is locked, use the username and password provided in the Login dialog box to unlock the CTC session.

For issues with RSA login, see the Troubleshooting with RSA, on page 39 section.

Step 6 Each time you log into an ONS 15454 or NCS 2000, you can select the following login options:

- Additional Nodes—Displays a list of current login node groups. To create a login node group or add additional groups, see the DLP-G48 Create Login Node Groups, on page 41.

- Disable Network Discovery—Check this box to view only the ONS 15454 or NCS 2000 (and additional nodes within the login node group, if any) entered in the Node Name field. Nodes linked to this node through DCCs are not discovered and will not appear in CTC network view. Using this option can decrease the CTC startup time in networks with many DCC-connected nodes, and can reduce memory consumption.

- Disable Circuit Management—Check this box to disable discovery of existing circuits. Using this option can decrease the CTC initialization time in networks with many existing circuits and reduce memory consumption. After you are logged in, you can enable circuit discovery at any time by choosing the Enable Circuit Discovery button on the Circuits tab.

Step 7 If you keep Disable Network Discovery unchecked, CTC attempts to upgrade the CTC software by downloading more recent versions of the JAR files it finds during the network discovery. Click **Yes** to allow CTC to download the newer JAR files, or **No** to prevent CTC from downloading the JAR files.

Note	Upgrading the CTC software will overwrite your existing software. You must restart CTC after the upgrade is complete.

Step 8 Click **Login**.

If the login is successful, the following appears:

- For the nodes with software R9.4 or earlier releases—The CTC node view window (in single-shelf mode) or multishelf view window (in multishelf mode) appears.

- For the nodes with software R9.6 or later releases—The CTC window opens a multi-tab view—Home Page, Network View, and Node View tabs appear. By default, the Node View tab is active for single-shelf nodes or Multishelf View tab is active for multishelf node.

From here, you can navigate to other CTC views to provision and manage the ONS 15454 or NCS 2000. If you need to turn up the shelf for the first time, see the chapter "Turn Up a Node" in the Cisco ONS 15454 DWDM Configuration Guide and Cisco NCS 2000 Series Network Configuration Guide. If login problems occur, refer to the Cisco ONS 15454 DWDM Troubleshooting Guide and Cisco NCS 2000 Series Troubleshooting Guide.

Step 9   Return to your originating procedure (NTP).

DLP-G Log into CTC with Stored Login Credentials

Purpose	(Only for super user) This task logs into the CTC with stored login credentials.
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3 One of the following procedures: • NTP-G18 Set Up CTC Computer for Local Craft Connection to the Node, on page 11 • NTP-G19 Set Up a CTC Computer for a Corporate LAN Connection to the Node, on page 28
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Super user

The user can store CTC login credentials in the local system so that the user can start the CTC session without the login credentials.

If the password is changed for Security user, the user needs to re-authenticate the node and store the login credentials.

If the user wants to save new Super user, it is recommended to start a new CTC session with new Super user and store the login credentials.

Procedure

Step 1   From the Edit menu in node view, choose **Preferences** > > **Login Store**.

Step 2   Click **Store** to securely store the login credentials in the local system and click **OK**.

The user name and password are stored in encrypted format in the CTC preferences file in the local system using AES 128-bit encryption with PKCS5Padding (Padded Cipher).

The strored login credentials are used to automatically start new CTC sessions.

CTC started with stored login credentials has default discovery of network and circuits. The user cannot check or uncheck the **Disable Network Discovery** and **Disable Circuit Management** check boxes.

Step 3   Close and re-open the Preferences window.

Step 4   (Display only) The **Credentials Stored Locally** check box is checked when the login credentials are securely stored.

Step 5 (Optional) Click **Clear** to clear the stored login credentials from the local system.

Step 6 Return to your originating procedure (NTP).

Troubleshooting with RSA

Table 3: RSA Troubleshooting Issues and Solutions

Category	Possible Issues	Solution
Provisioning issues	RSA license is not available	RSA is license based server. Contact the RSA team.
	Token licenses are invalid	RSA provides individual license based tokens. Check whether the token has valid licenses.
	Provisioning errors	Follow the RADIUS and RSA provisioning errors for the first time and confirm before enabling the RADIUS server on NE. When RADIUS server is enabled, you may be locked out if the Final Authenticator is not enabled.
	Node DCN, RADIUS, and RSA server connectivity issues	Check the node connectivity. See NTP-G229 Provisioning DCN Extension for a Network Using GCC/DCC and DLP-G281 Configure the Node for RADIUS Authentication for more information.
	Correct user ID mapping in RSA server	RSA tokens are individually associated with the user names in the RSA server. These names must be configured in the RADIUS server with appropriate privileges.
	GNE and ENE configurations	Perform the required GNE and ENE configurations before enabling RADIUS and RSA based authentication. See NTP-G212 Manually Provisioning a GNE/ENE to Manage an ENE using SNMPv3 and NTP-G213 Automatically Provisioning a GNE to Manage an ENE using SNMPv3 for GNE and ENE configurations.

Category	Possible Issues	Solution
Login authentication issues	Token locked by administrator and node lockout	RSA token can be controlled from RSA authentication server by enabling lock that disables the user.
	Token PIN is not provided by RSA. Token PIN must be provided by user.	RSA configuration issue. Contact RSA administrator to provision Token generated by RSA.
	Token failed due to sync issue	Re-sync the token with the RSA server. Contact RSA administrator.
Next token mode	Next token mode	This issue happens if you enter the wrong code multiple times. Enter the valid next token to be authenticated. If the next token is rejected by the RSA server, contact the RSA administrator. This issue may also happen if the token is out of sync. Re-sync the token with the RSA server. Contact RSA administrator.
Privilege issues	User privileges	RSA provides user privileges based on RADIUS server provisioning. RSA does not hold any privilege provisioning for tokens. RSA validates user authentication and privileges are assigned according to RADIUS configuration.

DLP-G47 Install Public-Key Security Certificate

Purpose	This task installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run Software Release 4.1 or later.
Tools/Equipment	None
Prerequisite Procedures	This task is performed during the DLP-G46 Log into CTC. You cannot perform it outside of this task.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

Note The Java Plug-in Security Warning dialog box options that appear depend on the JRE version you are using. If you installed JRE 1.6, you will see the following options: Yes, No, Always, and More Details. If you are using JRE 1.3.1_02, you will see the following options (shown in parentheses in the following list): Grant This Session, Deny, Grant Always, and View Certificate.

- Yes (Grant This Session)—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into the ONS 15454 and NCS 2000.

- No (Deny)—Denies permission to install the certificate. If you choose this option, you cannot log into the ONS 15454 and NCS 2000.

- Always (Grant Always)—Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.

- More Details (View Certificate)—Allows you to view the public-key security certificate.

Step 2 Return to your originating procedure (NTP) or task (DLP).

DLP-G48 Create Login Node Groups

Purpose	This task creates a login node group to display the nodes that have an IP connection but not a data channel connection (DCC) to the login node.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 From the Edit menu in node view, choose **Preferences**.

Step 2 Click **Login Node Group** and **Create Group**.

Step 3 Enter a name for the group in the Create Login Group Name dialog box. Click **OK**.

Step 4 In the Members area, type the IP address (or node name) of a node you want to add to the group. Click Add. Repeat this step for each node that you want to add to the group.

Note   If the ONS 15454, ONS 15454 M2, ONS 15454 M6, and NCS 2000 that you want to add to the login node group has TCC2P/TCC3/TNC/TNCE/TSC/TSCE cards installed and the TCC2P/TCC3/TNC/TNCE/TSC/TSCE secure mode option is enabled, enter the backplane LAN port (or EMS port) IP address. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 DWDM Configuration Guide* or Cisco NCS 2000 Series Network Configuration Guide for more information about secure mode.

Step 5   Click **OK**.

The next time you log into an ONS 15454 or NCS 2000, the login node group will be available in the Additional Nodes list of the Login dialog box. For example, in the following figure, a login node group is created that contains the IP addresses for Nodes 1, 4, and 5. During login, if you choose this group from the Additional Nodes list and Disable Network Discovery is not selected, all nodes in the figure appear. If the login group and Disable Network Discovery are both selected, only Nodes 1, 4, and 5 appear. You can create as many login node groups as you need. The groups are stored in the CTC preferences file and are not visible to other users.

Figure 1: Login Node Group
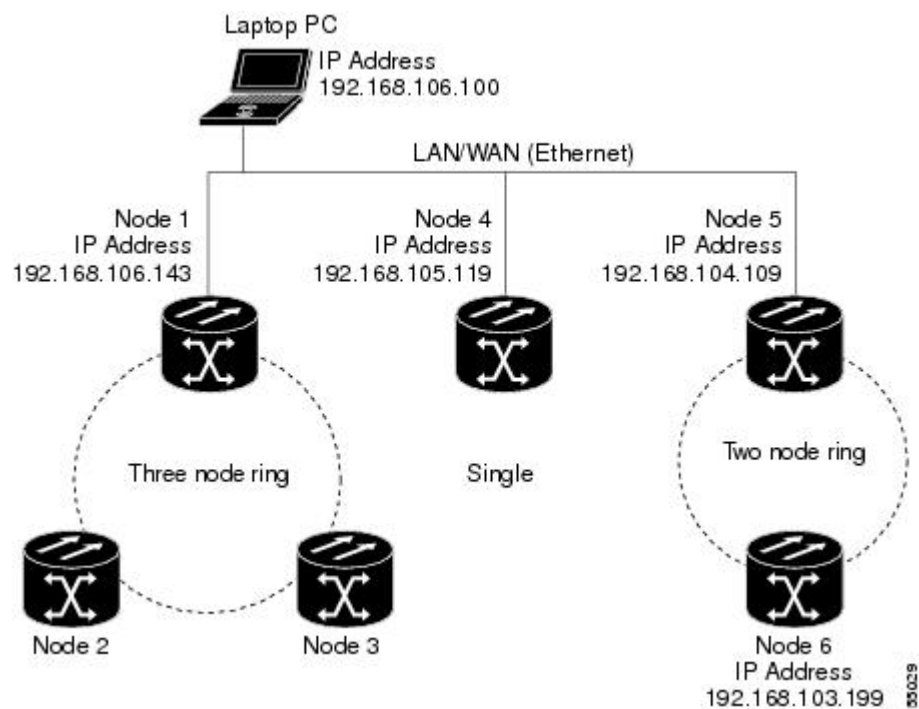
Step 6   Return to your originating procedure (NTP).

DLP-G49 Add a Node to the Current Session or Login Group

Purpose	This task adds a node to the current CTC session or login node group.

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

Procedure

Step 1 From the CTC File menu, click **Add Node**. The Add Node dialog box is displayed.

Step 2 In the Add Node dialog box, enter the node name (or IP address).

If the ONS 15454, ONS 15454 M2, ONS 15454 M6, and NCS 2000 that you want to add has TCC2P/TCC3/TNC/TNCE/TSC/TSCE cards installed and the TCC2P/TCC3/TNC/TNCE/TSC/TSCE secure mode option is enabled, enter the backplane LAN port IP address.

Note If the node is in secure mode, the backplane IP address display might be disabled. A Superuser can reenable the IP display. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. For more information about secure mode, see the "Management Network Connectivity" chapter in the Cisco ONS 15454 DWDM Configuration Guide or Cisco NCS 2000 Series Network Configuration Guide.

Step 3 If you want to add the node to the current login node group, check **Add to current login node group**. Otherwise, leave it unchecked.

Note This check box is active only if you selected a login group when you logged into CTC.

Step 4 (Cisco 7600 series router only) To add a Cisco 7600 node to the DWDM network, check **Add Cisco 7600 series router** and select the peer node from the drop-down list.

Note To view the **Add Cisco 7600 series router** option in the **Add Node** dialog box, add the attribute **"ctc.isC7600Supported=1"** in the /users/<username>/.ctcrc file. This should be done prior to launching CTC. By default, IPoDWDM using the Cisco 7600 series router is disabled.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-G50 Delete a Node from the Current Session or Login Group

Purpose	This task removes a node from the current CTC session or login node group. To remove a node from a login node group that is not the current one, see DLP-G51 Delete a Node from a Specific Login Node Group, on page 44 task.

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

Procedure

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

Step 2 On the network map, single-click the node that you want to delete.

Step 3 From the CTC File menu, click **Delete Selected Node**.

After a few seconds, the node disappears from the network view map.

Step 4 Return to your originating procedure (NTP).

DLP-G51 Delete a Node from a Specific Login Node Group

Purpose	This task removes a node from a specific login node group. To remove a node from the current login node group, see the .
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In any CTC view, from the CTC Edit menu, choose **Preferences.**

Step 2 In the Preferences dialog box, click the **Login Node Groups** tab.

Step 3 Click the login node group tab containing the node you want to remove.

Step 4 Click the node you want to remove, then click **Remove.**

Step 5 Click **OK**.

Step 6   Return to your originating procedure (NTP).

DLP-G53 Configure the CTC Alerts Dialog Box for Automatic Popup

Purpose	This task sets up the CTC Alerts dialog box to open for all alerts, for circuit deletion errors only, or never. The CTC Alerts dialog box displays network disconnection, Send-PDIP inconsistency, circuit deletion status, condition retrieval errors, and software download failure.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1   Click the **CTC Alerts** toolbar icon. (The icon is located on the far right of the CTC toolbar.)

Step 2   In the CTC Alerts dialog box, choose one of the following:

- All alerts—Sets the CTC Alerts dialog box to open automatically for all notifications.

- Error alerts only—Sets the CTC Alerts dialog box to open automatically for circuit deletion errors only.

- Never—Sets the CTC Alerts dialog box to never open automatically.

Step 3   Click **Close**.

Step 4   Return to your originating procedure (NTP).

DLP-G448 Designate SOCKS GNEs

Purpose	This task designates ONS 15454 or NCS 2000 GNEs that will serve as SOCKS servers to facilitate login performance in large networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

> **Note** This task cannot be completed until the ONS 15454 or NCS 2000 network has been provisioned. It is intended only for users experiencing long login times, and especially users with Windows XP, Service Pack 2.

> **Note** To complete this task, you will need a list of ONS 15454 or NCS 2000 (IP addresses or node names) that are provisioned as GNEs. You must have connectivity to the GNEs.

Procedure

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

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

Step 3   In the Designated SOCKS Server field, type the IP address or DNS node name of the first ONS 15454 or NCS 2000 SOCKS server. The ONS 15454 or NCS 2000 that you enter must have SOCKS proxy server enabled, and it must have LAN access.

Step 4   Click **Add**. The node is added to the SOCKS server list. If you need to remove a node on the list, click **Remove**.

Step 5   Repeat Steps Step 3 and Step 4to add all qualified ONS 15454 or NCS 2000 within the network. Add all ONS nodes that have SOCKS proxy enabled and are connected to the LAN.

Step 6   Click **Check All Servers**. CTC verifies that all nodes can perform as SOCKS servers. Once verified, a check is placed next to the node IP address or node name in the SOCKS server list. An X placed next to the node indicates one or more of the following:

- The entry does not correspond to a valid DNS name.

- The numeric IP address is invalid.

- The node cannot be reached.

- The node can be reached, but the SOCKS port cannot be accessed, for example, a firewall problem might exist.

Step 7   Click **Apply**. The list of ONS 15454 or NCS 2000 nodes, including ones that received an X in Step 4, are added as SOCKS servers.

Step 8   Click **OK** to close the Preferences dialog box.

Step 9   Return to your originating procedure (NTP).

NTP-G190 Use the CTC Launcher Application to Manage Multiple ONS Nodes

Purpose	This procedure uses the CTC Launcher to start a CTC session with an ONS NE that has an IP connection to the CTC computer; create TL1 tunnels to connect to ONS NEs on the other side of third-party, OSI-based GNEs; and view, manage, and delete TL1 tunnels using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3 One of the following procedures: • NTP-G18 Set Up CTC Computer for Local Craft Connection to the Node, on page 11 • NTP-G19 Set Up a CTC Computer for a Corporate LAN Connection to the Node, on page 28
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note   JRE 1.6 must be installed on the PC you are using with the CTC Launcher application.

Procedure

Step 1   As needed, complete one of the following tasks to install the CTC Launcher:

- DLP-G441 Install the CTC Launcher Application from a Node, on page 48
- DLP-G736 Install the CTC Launcher Application for a Node, on page 48

Step 2   As needed, complete the DLP-G442 Connect to Nodes Using the CTC Launcher, on page 49 task to connect to an ONS network element with direct IP connectivity.

Step 3   As needed, complete the DLP-G449 Install or Reinstall the CTC JAR Files, on page 56.

Step 4   As needed, complete one of the following tasks to create a TL1 tunnel, which enables you to connect to an ONS network element residing behind OSI-based, third-party GNEs:

- DLP-G443 Create a TL1 Tunnel Using the CTC Launcher, on page 50
- DLP-G444 Create a TL1 Tunnel Using CTC, on page 52

Step 5   As needed, complete the DLP-G445 View TL1 Tunnel Information, on page 53.

Step 6   As needed, complete the DLP-G446 Edit a TL1 Tunnel Using CTC, on page 55.

Step 7   As needed, complete the DLP-G447 Delete a TL1 Tunnel Using CTC, on page 56.

Stop. You have completed this procedure.

DLP-G441 Install the CTC Launcher Application from a Node

Note	This task is applicable for nodes with software R9.4 and earlier releases.

Purpose	This task installs the CTC Launcher from an ONS 15454 or NCS 2000 node.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1   Using a web browser, go to the following address, where node-name is the DNS name of a node you are going to access:

http://node-name/fs/StartCTC.exe

The browser File Download dialog box appears.

Step 2   Click **Save.**

Step 3   Navigate to the location where you want to save the StartCTC.exe file on the local hard drive.

Step 4   Click **Save.**

Step 5   Return to your originating procedure (NTP).

DLP-G736 Install the CTC Launcher Application for a Node

Purpose	This task installs the CTC Launcher for a node.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1   Using a web browser, go to the Download Software link.

Step 2   Click the **Optical Networking Systems (ONS) Utilities** link.

Step 3   Choose the cache installer file for the required release.

Step 4   Download the CacheInstall.kx.Rxxx.zip file.

       xxx indicates the release number.

Step 5   Navigate to the location where you want to save the CacheInstall.kx.Rxxx.zip file on the local hard disk.

Step 6   Click **Save**.

Step 7   Unzip the CacheInstall.kx.Rxxx.zip file.

Step 8   Double Click the SetupCtc-xxx file.

       This creates a directory named SetupCtc-xxx, which contains the StartCtc file, LD cache, and few JAR files.

Step 9   Return to your originating procedure (NTP).

DLP-G442 Connect to Nodes Using the CTC Launcher

Purpose	This task adds a node to the current CTC session or login node group.
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1   Start the CTC Launcher:

- Windows: navigate to the directory containing the StartCTC.exe file and double-click it. (You can also use the Windows Start menu Run command.)
- Solaris: assuming the StartCTC.exe file is accessible from the current shell path, navigate to the directory containing the StartCTC.exe file and type:

% java -jar StartCTC.exe

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

Step 3 In the Login Node box, enter the ONS NE or NCS 2000 node name or IP address. (If the address was entered previously, you can choose it from the drop-down menu.)

Step 4 Select the CTC version you want to launch from the following choices in the drop-down menu:

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

Note Cisco recommends that you always use the "Same version as the login node" unless the use of newer CTC versions is needed (for example, when CTC must manage a network containing mixed version NEs).

Step 5 Click **Launch CTC**. After the connection is made, the CTC Login dialog box appears.

Step 6 Log into the ONS 15454 or NCS 2000 node.

Note Because each CTC version requires particular JRE versions, the CTC Launcher will prompt the user for the location of a suitable JRE whenever a new CTC version is launched for the first time using a file chooser dialog (if a suitable JRE version is not known by the launcher yet). That JRE information is then saved in the user's preferences file. From the selection dialog, select any appropriate JRE directory.

After the JRE version is selected, the CTC will be launched. The required jar files will be downloaded into the new cache if they are missing. The CTC Login window will appear after a few seconds.

Step 7 Return to your originating procedure (NTP).

DLP-G443 Create a TL1 Tunnel Using the CTC Launcher

Purpose	This task creates a TL1 tunnel using the CTC Launcher, and the tunnel transports the TCP traffic to and from ONS ENEs through the OSI-based GNE.
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1   Double-click the StartCTC.exe file.

Step 2   Click **Use TL1 Tunnel**.

Step 3   In the Open CTC TL1 Tunnel dialog box, enter the following:

- Far End TID—Enter the TID of the ONS ENE at the far end of the tunnel. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.

- Host Name/IP Address—Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS node through an OSI DCC network. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.

- Choose a port option:

  - Use Default TL1 Port—Choose this option if you want to use the default TL1 port 3081 and 3082.

  - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.

- TL1 Encoding Mode—Choose the TL1 encoding:

  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient encoding mode. However, you must verify that the GNE supports LV + Binary Payload encoding.

  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.

  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.

- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.

- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 4   Click **OK**.

Step 5   If the GNE Login Required box is checked, complete the following steps. If not, continue with the next step.

   a)   In the Login to Gateway NE dialog box UID field, enter the TL1 user name.

   b)   In the PID field, enter the TL1 user password.

   c)   Click **OK**.

Step 6   When the CTC Login dialog box appears, complete the CTC login.

Step 7   Return to your originating procedure (NTP).

DLP-G444 Create a TL1 Tunnel Using CTC

Purpose	This task creates a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click **Create.**

Step 3 In the Create CTC TL1 Tunnel dialog box, enter the following:

- Far End TID—Enter the TID of the ONS ENE at the far end of the tunnel. The ENE must be a Cisco ONS NE. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.

- Host Name/IP Address—Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.

- Choose a port option:

  - Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.

  - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.

- TL1 Encoding Mode—Choose the TL1 encoding:

  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.

  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.

  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.

- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.

• TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 4   Click **OK**.

Step 5   If the GNE Login Required box is checked, complete the following steps. If not, continue with next step.

    a)   In the Login to Gateway NE dialog box UID field, enter the TL1 user name.

    b)   In the PID field, enter the TL1 user password.

    c)   Click **OK**.

Step 6   After the CTC Login dialog box appears, log into CTC.

Step 7   Return to your originating procedure (NTP).

DLP-G445 View TL1 Tunnel Information

Purpose	This task views a TL1 tunnel created using the CTC Launcher.
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Procedure

Step 1   Log into CTC, See DLP-G46 Log into CTC.

Step 2   From the Tools menu, choose **Manage TL1 Tunnels**.

Step 3   In the TL1 Tunnels window, view the information shown in the following table.

Table 4: TL1 Tunnels Window

Item	Description
Far End TID	The Target ID of the NE at the far end of the tunnel. This NE is an ONS NE. It is typically connected with an OSI DCC to a third-party vender GNE. CTC manages this NE.
GNE Host	The GNE host or IP address through which the tunnel is established. This is generally a third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.

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

Step 4   Return to your originating procedure (NTP).

DLP-G446 Edit a TL1 Tunnel Using CTC

Purpose	This task edits a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click the tunnel you want to edit.

Step 3 Click **Edit.**

Step 4 In the Edit CTC TL1 Tunnel dialog box, edit the following:

- Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
- Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
    - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
    - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
    - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 5 Click OK.

Step 6 If the GNE Login Required box is checked, complete login in the Login to Gateway NE dialog box. If not, continue the next step.

a) In the UID field, enter the TL1 user name.
b) In the PID field, enter the TL1 user password.
c) Click OK.

Step 7 When the CTC Login dialog box appears, complete the CTC login. Refer to login procedures in the user documentation for the ONS ENE.

Step 8 Return to your originating procedure (NTP).

DLP-G447 Delete a TL1 Tunnel Using CTC

Purpose	This task deletes a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click the tunnel you want to delete.

Step 3 Click **Delete.**

Step 4 In the confirmation dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-G449 Install or Reinstall the CTC JAR Files

Purpose	This task installs or reinstalls the CTC JAR files into the CTC cache directory on your PC. This is useful when you are using a new CTC version and want to install or reinstall the CTC JAR files without logging into a node or using the StartCTC application (StartCTC.exe).
Tools/Equipment	None
Prerequisite Procedures	NTP-G17 Set Up Computer for CTC, on page 3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1 Insert the Cisco ONS 15454 or Cisco ONS 15454 SDH Software CD into your CD drive.

Step 2 Navigate to the CacheInstall directory.

Step 3 Copy the SetupCtc-version.exe file to your local hard drive. Use any location that is convenient for you to access, such as the Windows desktop. Ensure that you have enough disk space to copy and extract the SetupCtc-version.exe file.

Step 4 Double-click the SetupCtc-version.exe file. This creates a directory named SetupCtc-version (at the same location), which contains the LDCACHE.exe file and other CTC files.

Step 5 Double-click the LDCACHE.exe file to install or reinstall the new CTC JAR files into the CTC cache directory on your PC.

Step 6 Return to your originating procedure (NTP).

DLP-G450 Configuring Windows Vista or Windows 7 to Support CTC

Purpose	This task describes the configurations that must be done in Windows Vista or Windows 7 operating system prior to launching CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1 Complete the following steps to disable Internet Explorer 7 protected mode:

Note Perform a full installation of the Windows Vista or Windows 7 operating system on your computer. If Windows Vista or Windows 7 is installed through operating system upgrade, CTC will not work. Refer to the manufacturer's user guide for instructions on how to install Windows Vista or Windows 7.

Note This procedure is needed only if CTC is launched from the Internet Explorer browser. If you start CTC by downloading the CTC Launcher application from the node, perform the DLP-G441 Install the CTC Launcher Application from a Node, on page 48

a) Open Internet Explorer

b) Click **Tools > Internet Options**.

c) Click the **Security** tab.

d) Select the zone that is appropriate. The available options are: Local Intranet, Internet, and Trusted Sites.

e) Check the **Disable Protect Mode** check box.

Step 2 Complete the following steps to Disable TCP Autotuning:

a) From the Windows Start menu, click **Search > Search for Files and Folders**. The Search window appears.

b) On the right side of the window in the Search box, type **Command Prompt** and press **Enter**. Windows will search for the Command Prompt application and list it in the search results.

c) Right click **cmd** and select **Run as administrator**.

d) Enter the administrator user ID and password and click **OK**.

e) A Command prompt windows appears. At the command prompt enter the following text:

```
netsh interface tcp set global autotuninglevel=disabled
```

Autotuning can be enabled if desired using the following command:

```
netsh interface tcp set global autotuninglevel=normal
```

Step 3 Download and install the CTC cache from the following link (Select the correct release from the utilities).https://software.cisco.com/download/home/283307670/type

Step 4 Return to your originating procedure (NTP).

NTP-G323 Create or Delete a Perspective View

Purpose	This procedure is used to create or delete a perspective view in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1 Complete the following as required:

• To Add a Perspective complete Step 2, on page 59

• To Remove a Perspective complete

Step 2   To add a perspective:

a) Choose **Window > Perspective > Add Perspective**. The Create New Perspective dialog box opens. Alternatively, you can open the dialog box by clicking the Add Perspective tool in the toolbar.

b) Enter the name of the perspective in the Perspective name field.

c) In the Tab Selection area, check the tab check boxes that you want to include in the perspective. The available tab options are Alarms, Conditions, History, Circuits, Provisioning, Inventory, Performance, Layer2+, and Maintenance. Based on the view some of the options are unavailable.

d) (Mandatory) In the Node Selection area, select the node you want to include in the perspective.

e) In the Map Selection area, click the Network View or Functional View (MSTP only) radio button.

f) Check the Attach Network Explorer check box to attach the network explorer to the perspective.

It is useful to add the network explorer in the newly created perspective. To see the network explorer in any perspective, press Ctrl-N.

Step 3   To remove a perspective:

a) Choose **Window > Perspective > Remove Perspective**. The Remove Perspective dialog box opens. Alternatively, you can open the dialog box by clicking the Remove Perspective tool in the toolbar.

b) Select the perspective you want to delete from the list available. To select multiple perspectives, press the Ctrl and select the perspectives. Click Select All to select all the perspectives.

c) Click **Delete** to delete the selected perspectives.

Note   The default view cannot be deleted.

d) Click cancel to **Cancel** the selection.

Step 4   In any particular perspective choose **Window > Perspective > Remove Active Perspective** to remove the present active view. Alternatively, you can remove the active view by clicking the Remove Active Perspective tool in the toolbar.

Note   In the default view, Remove Active Perspective option is unavailable.

Stop. You have completed this procedure.

NTP-G336 Persist a Perspective View

Purpose	This procedure is used to persist a perspective view in CTC.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC • NTP-G323 Create or Delete a Perspective View, on page 58
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	None

Procedure

Step 1 Choose **Edit > Preferences > Perspective**.

Step 2 Check the **Enable Persistence** check box to enable persistence of a perspective view.

Step 3 Enter the number of perspective views you want to be persisted in the Max Persistence field.

For example, if you enter 5 in the Max Persistence field, you can create four perspective views which can be persisted. The default CTC Perspective view is also included.

Step 4 Enter **persistence** in the Persistence File field.

Do not enter any other name. The persistence details of the perspective views are stored in the perspective.xml file.

Stop. You have completed this procedure.

Additional References

Related Documents

Use this document in conjunction with the other release-specific documentation listed in this table:

Link	Description
Cisco ONS Documentation Roadmap	Provides quick access to publications of Cisco ONS releases.
Cisco ONS 15454 DWDM Control Card and Node Configuration Guide	Provides background and reference material and procedures for installation and configuration of control cards and node configuration on Cisco ONS 15454 dense wavelength division multiplexing (DWDM) systems.
Cisco ONS 15454 DWDM Line Card Configuration Guide	Provides background and reference material and procedures for installation and configuration of line cards on Cisco ONS 15454 dense wavelength division multiplexing (DWDM) systems.
Cisco ONS 15454 DWDM Network Configuration Guide	Provides background and reference material, procedures for turn up, provisioning, and maintenance of Cisco ONS 15454 dense wavelength division multiplexing (DWDM) systems.
Cisco ONS 15454 DWDM Troubleshooting Guide	Provides general troubleshooting instructions, alarm troubleshooting instructions, and a list of error messages that apply to the Cisco ONS 15454 dense wavelength division multiplexing (DWDM) systems.

Link	Description
Release Notes for Cisco ONS 15454	Provides information about new features and enhancements for the Cisco ONS 15454 DWDM platforms.
Cisco ONS 15454 Hardware Installation Guide	Provides installation information of the Cisco ONS 15454 hardware.
Cisco ONS 15454 DWDM Licensing Guide	Provides information about installing and managing Cisco ONS 15454 DWDM licenses.
Cisco ONS SDH TL1 Command Guide *Cisco ONS SONET TL1 Command Guide*	Provides a comprehensive list of TL1 commands.
Installing the GBIC, SFP, SFP+, XFP, CXP, CFP, and CPAK Optical Modules in Cisco ONS Platforms	Provides information about the Pluggable Port Modules support.

Link	Description
Cisco NCS 2000 Series Documentation Roadmap	Provides quick access to publications of Cisco NCS 2000 Series releases.
Cisco NCS 2000 Series Control Card and Node Configuration Guide	Provides background and reference material and procedures for installation and configuration of control cards and node configuration on Cisco NCS 2000 Series systems.
Cisco NCS 2000 Series Line Card Configuration Guide	Provides background and reference material and procedures for installation and configuration of line cards on Cisco NCS 2000 Series systems.
Cisco NCS 2000 Series Network Configuration Guide	Provides background and reference material, procedures for turn up, provisioning, and maintenance of Cisco NCS 2000 Series systems.
Cisco NCS 2000 Series Troubleshooting Guide	Provides general troubleshooting instructions, alarm troubleshooting instructions, and a list of error messages that apply to the Cisco NCS 2000 Series systems.
Release Notes for Cisco NCS 2000 Series	Provides information about new features and enhancements for the Cisco NCS 2000 Series systems.
Cisco NCS 2000 Series Hardware Installation Guide	Provides installation information of the Cisco NCS 2000 Series hardware.
Cisco NCS 2000 Series Licensing Configuration Guide	Provides information about installing and managing NCS licenses.
Cisco NCS 2000 Series TL1 Command Guide	Provides a comprehensive list of TL1 commands.
Installing the GBIC, SFP, SFP+, XFP, CXP, CFP, and CPAK Optical Modules in Cisco NCS Platforms	Provides information about the Pluggable Port Modules support.

Technical Assistance

Link	Description
http://www.cisco.com/support	The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.
	To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.
	Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.

Short Description

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.