

Cisco ONS 15454 Frequently Asked Questions

Document ID: 46249

Questions

Introduction
Alarm
Cross-Connect (XC)
Cisco Transport Controller (CTC)
Data Communications Channel (DCC)
Ethernet
IP Routing and Static Routes
Power Supply
Protection Groups
Provisioning
Timing
Transaction Language 1 (TL1)
VPN
Simple Network Management Protocol (SNMP)
Related Information

Introduction

This document provides answers to some common questions about the Cisco ONS 15454 Optical Transport Platform.

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Alarm

Q. I have Signal Label Mismatch Failure (SLMF) Unequipped-Path (UNEQ-P) alarms reported on the optical card(s), or an alarm indication signal (AIS) alarm on the terminating cards. How do I clear these alarms?

A. Consider these options to clear these UNEQ-P alarms:

- ◆ SLMF UNEQ-P alarms usually indicate that there is no signal present on the specified Synchronous Transport Signal (STS) or Virtual Tributary (VT). If you have created a new circuit that does not have a signal on it yet, you receive a UNEQ-P alarm on the optical cards and an Alarm Indication Signal Path (AIS-P) alarm on the terminating cards. If this is a working circuit, verify whether the equipment external to the Cisco ONS 15454 works properly.
- ◆ Another possibility is that you have an empty VT Tunnel. If you have either built a tunnel and have not added any VT1.5s, or have deleted all the VT1.5s from an existing tunnel, UNEQ-P alarms can occur.
- ◆ If you have complete visibility to all network elements (NEs), check for incomplete circuits. These could represent stranded bandwidth from circuits that were not completely deleted. If you find incomplete circuits, verify whether they are active

circuits that still pass traffic. If the circuits are not needed or do not pass traffic, delete them, and log out of Cisco Transport Controller (CTC). Log back into CTC, and check for incomplete circuits again. Re-create any needed circuits.

- ◆ In the case of TL1 like and true TL1 cross connects, this alarm can be displayed when building the individual cross connects in the nodes. It is normal to see UNEQ-P when cross connects are present in one NE but are absent on the same time slot on an adjacent NE.

Q. Why does the DS3 card not report Alarm Indication Signal-Path (AIS-P) alarms from external equipment?

A. The DS3 card terminates the signal on the ports at the backplane. To check the Performance Monitoring (PM) data on a DS3 from an external device, check the PM data on the OCn that is cross-connected to the DS3 circuit. This enables you to monitor any path-level errors that come in on the DS3 signal.

Q. There is a blue alarm that indicates holdover synchronization mode. What does this alarm mean?

A. This alarm indicates that the clock runs at the frequency of the last known good timing reference input. The alarm is triggered when the last timing reference input fails.

Note: The Cisco ONS 15454 supports holdover timing per GR-4436 when provisioned for external (BITS) timing.

Q. There is a major alarm that indicates freerunning synchronization mode. What does this alarm mean?

A. This alarm indicates that the clock uses the internal oscillator as its only timing frequency reference. This occurs when there is no reliable prior timing reference information to use.

Cross-Connect (XC)

Q. I am unable to create Virtual Tributary (VT) 1.5 circuits in Cisco Transport Controller (CTC), and I get the error message Error while finishing circuit creation. Unable to provision circuit. Unable to create connection object at <node name>. What does this mean?

A. This error message indicates that you have possibly run out of bandwidth on the VT Cross-Connect (XC) matrix at the node name included at the end of the message. The matrix has a maximum capacity of 336 bidirectional VT 1.5 circuits in BLSR, and 224 bidirectional VT1.5s in UPSR, if you assume efficient VT1.5 grooming. For important information on VT use, refer to Section 9.2 of the Cisco ONS 15454 Reference Manual, Release 5.0. Also, refer to Understanding the 15454 XC and XC-VT Switching Matrix for an in-depth explanation of how the XC matrix works.

From release 4.1 onwards, VT and STS matrix resources are tracked and reported. You can find this information under the **Maintenance/Cross Connect** tab of CTC. For more information refer to Cisco ONS 15454 Reference Manual, Release 5.0, Section 10.2

Q. Some unused circuits were deleted while they were incomplete. It could have stranded some of the circuit spans. How do I check for and delete stranded circuits with Transaction Language 1 (TL1)?

A. Complete these steps to check for and delete stranded circuits:

1. Log into TL1 (see Section 12 of the Cisco ONS 15454 and ONS 15327 TL1 Command Quick Reference Guide, Release 4.0). For this, you must issue the **ACT USER::TID:<userid>(CTAG)::<passwd>**; command.
2. Issue the **(RTRV-CRS-<STS-PATH OR VT1>::(TID):<sts_ep or vt>:(CTAG)::,,;** command to verify the stranded circuits.
3. If the stranded circuit is still in the system, issue the **(DLT-CRS-<STS-PATH OR VT1>::(TID):<from>,<to>:(CTAG)::;** command to delete the circuit.

Q. How do I avoid Virtual Tributary (VT) Cross-Connect (XC) exhaustion through VT tunneling?

A. When the source VT is at least two hops away from the destination, you can use a VT tunnel to free VT-XC resources in the pass through node(s). In essence, the tunnel keeps the VT 1.5s from being demuxed from the transport Synchronous Transport Signal (STS) at each pass-through node between the source and destination. This tunnel (STS) is reused whenever another VT is created with the source and destination nodes inside the boundaries of an existing tunnel. The tunnel is available to any subsequent VTs until the transport STS is exhausted.

Note: Pass-through nodes do not need XC-VT cards. They only need XC cards to perform this function.

For an in-depth explanation of how the XC-VT matrix works, refer to Understanding the 15454 XC and XC-VT Switching Matrix.

Cisco Transport Controller (CTC)

Q. When I try to provision a remote Cisco 15454 network element (NE) that shows up in Network view in CTC, why is the NE icon gray? Why does it show only the IP address and not the node name? Also, why does the node return the error message `Node not initialized` when I attempt to log in?

A. These symptoms can be generated by one of these causes:

- ◆ There is no proper IP route between the remote NE and the Cisco Transport Controller (CTC) client.
- ◆ The username and password used to log in to the local NE are different from the ones on the remote NE. For network-level access to all nodes, all nodes must use the same username and password.
- ◆ If the software revision is 3.3 or later, you must enable the Proxy Server feature.

For specific information on IP routing and how to troubleshoot, refer to Chapter 11: IP Networking of the Cisco ONS 15454 Reference Manual, Release 5.0.

Q. I can ping the Cisco ONS 15454 network element (NE), but Cisco Transport Controller (CTC) does not launch from the browser, although I have loaded the appropriate Java" Runtime Environment (JRE), and have executed the javapolicyinstall.bat file. How do I correct this problem?

A. Try any of these suggestions to correct this problem:

- ◆ If the computer has been used previously to connect to Cisco ONS 15454 NEs, delete the Java" Archive (JAR) files in the C:\Temp directory, and reboot the computer.
- ◆ If the PC is connected directly to a Cisco ONS 15454 unit, verify whether your browser is configured correctly.

Complete these steps to verify whether your browser is configured not to use a Proxy server to access the the Internet:

1. In Netscape, select **Edit > Preferences > Advanced > Proxies**.
2. Verify whether the Proxies configuration is set to **Direct connection to the Internet**.
3. In Internet Explorer, select **Tools > Internet Options > Advanced > HTTP 1.1 Settings**.
4. Ensure that the **Use HTTP 1.1 through proxy connections** option is not checked.
5. Temporarily disable any virus-scanning software on the computer.
6. Ensure that the computer has only one IP address assigned to it. The method to do this varies based on the system platform and operating system.
7. Reload the appropriate version of JRE and the **javapolicyinstall.bat** file onto the computer. For information on JRE compatibility, see Cisco ONS 15454 Reference Manual, Release 5.0.
8. Open the **Java Plug-in Control** panel. In order to do so:
 - a. Select **Start > Programs**.
 - b. On the **Advanced** tab, select **JRE1.3.1 in C:\Program**, and close the control panel.

Q. When I type the IP address in the location or address bar of the browser, the error message Unable to launch CTC due to applet security restrictions is displayed. How do I correct this problem?

A. Ensure that you have executed the **javapolicyinstall.bat** file on the Cisco ONS 15454 software CD. This procedure is described in the Cisco ONS 15454 Procedure Guide, Release 5.0.

If you have executed the .bat file, but still get the error message, you must manually edit the java.policy file on your computer. Complete these steps:

1. Search your computer for the .bat file (You can use the Windows Search or Find function).
2. Open the file with a text editor such as Notepad or WordPad.
3. Scroll to the end of the file and verify that these lines are present:

```
// Insert this into the system-wide or a per-user java.policy file. //
DO NOT OVERWRITE THE SYSTEM-WIDE POLICY FILE--ADD THESE LINES!
grant codeBase "http://*/fs/LAUNCHER.jar"
{permission java.security.AllPermission;};
```

4. If these lines are not in the file, add them manually and save the file. If these lines already appear in the file, verify whether they are complete and accurate, then save and close the file.

5. Close your browser.
6. Open a new browser window. Cisco Transport Controller (CTC) must now launch correctly.

If you still receive the error message after you complete these steps, save the **java.policy** file as a new file called **.java.policy**.

Note: Make sure to include the **.** at the beginning of the new file name.

Note: On PCs with Windows 95 or 98, save the file to the C:\Windows folder. On PCs with Windows NT 4.0, save the file to all of the user folders (for example, C:\WinNT\Profiles\JohnDoe).

Q. Why am I unable to see remote network elements (NEs) in the Network view of Cisco Transport Controller (CTC)? The NE icons do not show up at all.

A. Try these suggestions to correct this problem:

- ◆ Verify whether all of the OCn trunk cards have SONET Data Communications Channel (SDCC) terminations provisioned. Check whether all of the OCn trunk card ports are provisioned in-service. If there are Loss of Signal (LOS) alarms on the OCn trunk cards, there is either a fiber cable problem, or one or more failed OCn cards.
- ◆ It is possible that all of the NE icons are tiled on top of each other, especially if this is the first time you use the PC to log in to the network of NEs. In order to verify whether there is more than one NE icon, you need to move the top NE icon to a different location in the GUI. Use the drag and drop method to do so.

Note: The drag and drop method:

Hold down the **Ctrl** key and use the single mouse click button to click and hold. Move the mouse to the desired position and release the button.

Q. I have connectivity problems to a network element (NE). A popup window indicates Lost connection to node, changing to network view. There is also an alarm in Cisco Transport Controller (CTC) that indicates Loss of Connectivity between Node and CTC. What are the causes of these problems?

A. This can happen when the IP connection to the node to which you were connected is broken. There are several conditions which can cause this:

- ◆ If the active Timing Control Card (TCC) resets, the stand-by TCC activates, and IP connectivity is broken. This ends the session in that node.

Log out and restart CTC.

- ◆ Another possible cause is an incorrect static route configuration in a node within the network. In software versions 2.2.x, Proxy Address Resolution Protocol (ARP) is used for inter-nodal communication. If there is more than one node that tries to Proxy for the network, there can be contention in the network for Proxy. This can cause a shift in the IP routing among the nodes in the network, and break any existing IP connections.

Log out and restart a new CTC session.

- ◆ The most common problem is with the Data Communications Network (DCN). This is the network between your PC and the NE. Verify whether you can ping the NE from your PC, and that you get a decent ping time (less than 10ms is good), and that you receive no "request timed out" messages.

Q. How do I add additional network elements (NEs) that are not connected by way of optics (no Data Communications Channel (DCC) connectivity) to my Cisco Transport Controller (CTC) Network view?

A. You can add additional NEs with the help of multiple topology host files.

In software versions earlier than 3.x:

CTC can support the management of multiple rings or nodes that are not interconnected by fiber or SONET DCC (SDCC). This is accomplished by a cms.ini file that already resides where the cms.jar file is located. CMS automatically creates this file the first time it is launched. Currently, you must edit this file to support the multiple ring or node ability. Here is an example of the cms.ini (or .cmsrc) file with multiple nodes specified.

```
#CMS
Preferences File #Tue Aug 10 15:00:27 PDT 1999
Topology.Hosts=192.168.106.119\n192.168.106.109\n192.168.106.143
CMS_LAUNCHER.CmsJarPath=C:\\TEMP\\CMS63812.jar
CMS.LastHost=192.168.106.143
```

Note: The NE host names are separated by a \n (textual version of a new line). This file is not intended to be editable, though there currently is no way to enter multiple nodes other than by manual editing. Do not edit this file while you are logged in with CMS, because it can over-write. All other lines in the cms.ini file must not be edited.

In software version 3.x and later:

CTC can support the management of multiple rings or nodes that are not interconnected by fiber or SDCC. In order to accomplish this, create Login Node Groups under **Edit > Preferences > Login Node Groups** in the CTC menu.

Q. When I attempt to launch Cisco Transport Controller (CTC) to a network element (NE), why does the login initialization window hang at Checking software version compatibility?

A. Assume that you have already loaded the appropriate Java" Runtime Environment (JRE) version and the policy file to your PC. Java is probably active in the background. When you launch the CTC from your PC, the Timing Control Card (TCC) compares its .jar file to the .jar file located on the cache of the PC. During this time, the node either detects the correct version, and continues to run the program, or begins to download the proper version of CTC. This process takes a few minutes.

Q. How do I change the background image from the map of the United States to an image of my choice?

A. The procedure varies based on the software installed.

Complete these steps for Release 2.2x:

1. Edit the cms.ini file to include a line similar to this:
CmsNetwork.Map=/download/usphy.gif Make sure that the line is entered exactly as it appears above (case sensitive). This example is for a gif file located on a C: drive in the directory called download. This is located off the C: root, and the gif file is called **usphy.gif**.

Note: If you had a file called **state.gif** located on the C: drive in the directory called picture, you would enter the this:

Note: CmsNetwork.Map=C:\\picture\\state.gif

2. If, for example, you changed the map to an image of California, you would then have to change the top/bottom latitude, and left/right longitude to frame the new image. Therefore, for California, you would add these lines to the cms.ini file:
CmsNetwork.LeftLong=126.51 CmsNetwork.RightLong=117.41
CmsNetwork.TopLat=40.8 Cms Network.BottomLat=36.6 The numbers associated with these lines vary based on the image used.

For Release 3.x and later, you can do this through **Edit > Preferences > Map** in the CTC menu.

Q. Why do I repeatedly lose my connection to the network of network elements (NEs) in the Cisco Transport Controller (CTC)? The nodes turn gray, then back to color.

A. It is possible that the nodes do not have their IP addresses configured properly. If you are unable to establish connectivity, perform standard network/LAN diagnostics. For example, trace the IP route, check cables, and check any routers between the node and CTC. Cisco ONS 15454 IP addressing generally has seven common IP addressing scenarios or configurations. For detailed IP address scenarios, refer to Chapter 11: IP Networking in the Cisco ONS 15454 Reference Manual, Release 5.0.

Also, for a detailed explanation of how to configure routing on the Cisco ONS 15454, refer to Common Issues With IP Addressing and Static Routes on the 15454. From Release 2.2.0 onwards, LAN devices no longer need host routes to communicate with other Cisco ONS 15454s on the same subnet that connect through the Data Communications Channel (DCC).

A second possibility is that the SONET DCC (SDCC) does not function properly.

If CTC reports an Embedded Operations Channel (EOC) alarm, complete these steps to restore the SDCC:

1. If there is a Loss of Signal (LOS) alarm reported, first troubleshoot the LOS alarm.
2. On the node that reports the alarm, check the physical connections of the optic fibers configured to carry DCC traffic.
3. Verify whether both ends of the fiber span have in-service ports.
4. Verify whether both ends of the fibers have DCC provisioned.
5. Under the Node view, click the **Provisioning** tab and the **SONET DCC** subtab.

If the slot and port are listed under SDCC Terminations, the DCC is provisioned.

6. If the slot and port are not listed under the SDCC Terminations, click **Create**.
7. Click the optical card that links to the adjacent NE.
8. Click **OK**.

9. Repeat Steps 5 through 8 at the adjacent nodes.
10. Verify whether the OCn port is active and in-service.
11. With a test set, check for signal failure on fiber terminations.
12. Measure power levels to ensure that the budget loss is within the parameters of the receiver.
13. Make sure fiber connectors are securely fastened and properly terminated.
14. Restart the active TCC.
15. Select the **Provisioning** tab, and the **SONET DCC** subtab.
16. Delete the offending SDCC termination and create it again.
17. Verify whether both ends of the SDCC have been created again at the optical ports.

Q. How many concurrent Cisco Transport Controller (CTC) sessions can run on a single Cisco ONS 15454 and on a network of ONS 15454s?

A. In Release 2.2.x, it is recommended that you run only two concurrent CTC sessions per node. Release 3.x and later can handle up to five concurrent CTC sessions. CTC performance can vary, based on the volume of activity in each session, network bandwidth, TCCx card load and the size of the DCC connected network.

Q. What are the blue alarms in the Cisco Transport Controller (CTC) alarm browser?

A. The blue alarms are not really alarms at all. They are conditions. They display the condition of certain facilities, such as timing facilities, and there is no alarm severity associated with them.

Note: In CTC version 3.0 and later, and Cisco Transport Manager (CTM) version 2.1, the blue conditions do not appear in the alarm browser. They can be retrieved in a new browser called the Conditions browser.

Q. Does the Cisco Transport Controller (CTC) work through a firewall?

A. Yes, from release 3.0 onwards, you can set the Inter-ORB Protocol (IIOP) Listener port on the Cisco ONS 15454 and the CTC Workstation to enable communication through a firewall. For further details, refer to NTP-A 27 in the Cisco ONS 15454 Procedure Guide, Release 5.0.

Q. When I log into a Cisco ONS 15454 network element (NE) and navigate to the Network view of Cisco Transport Controller (CTC), the other nodes show up gray with the NE name, but I cannot log into them. I see the CTC user not authenticated on the TCC alarm in the GUI. What causes this alarm?

A. The CTC username and password used to log into the local NE are different from the ones required to log into the other NEs. For network access to all NEs, CTC usernames and passwords must be added to each node. Users are not automatically added to the other network NEs.

Q. Why do I have problems when I launch the Cisco Transport Controller (CTC) on my Windows 2000 PC?

A. Here are the possible problems associated with the launch of CTC on a Windows 2000 PC.

- ◆ It can take up to 30 minutes for Java to launch for the first time on a Windows 2000 PC. This is the only known issue with the launch of CTC on Windows 2000.
- ◆ It can be an IP problem. Issue the **ping** command to verify whether your PC has a good physical connection to the network element (NE).
- ◆ You need to run the **javapolicyinstall.bat** script located under the Windows directory on the Cisco ONS 15454 software CD if you get the error message `applet security restriction`.
- ◆ Reinstall the appropriate java version for the software you run. You can find this information in the ONS15454 Reference Guide for your release.
- ◆ If you receive the error message "applet not Inited", run the **javapolicyinstall.bat** script located under the Windows directory of the Cisco ONS 15454 software CD.

Data Communications Channel (DCC)

Q. What are DCC tunnels used for, and how do I create them?

A. A DCC is a Data Communications Channel. It is contained within section and line overhead, and is used as an Embedded Operations Channel (EOC) to communicate between network elements (NEs). You can use the Line DCCs (LDCCs) and the SONET DCCs (SDCCs) (when the SDCC is not used for Cisco ONS 15454 DCC terminations) to tunnel third party SONET equipment SDCCs across Cisco ONS 15454 networks.

In order to create a DCC tunnel, you connect the tunnel end points from one Cisco ONS 15454 optical port to another. Traffic is forwarded transparently, byte-for-byte, across the ONS 15454 network. For more details, refer to the most recent user documentation.

In order to build a DCC tunnel, refer to the appropriate version of the Cisco ONS15454 Procedure Guide. This depends upon the version of ONS15454 software you run.

Q. What causes the SDCC termination failure alarms alarm on my Cisco Transport Controller (CTC) alarm browser?

A. The Cisco ONS 15454 has lost its Data Communications Channel (DCC). The Cisco ONS 15454 uses the DCC on the SONET section layer (SDCC) to communicate network management information. The possible causes are:

- ◆ One or both ends of the fiber span are not in service.
- ◆ The far end of the fiber span does not have a DCC termination provisioned.
- ◆ There is signal failure on the fiber span (must be accompanied by Loss of Signal (LOS) alarms), broken or dirty connectors, loss budget out of parameters, improper termination, or a broken fiber.
- ◆ High Bit Error Rates (BERs) or a BER threshold for signal degrade alarm can sometimes cause this alarm.

Ethernet

Q. What is the difference between stitched and unstitched Ethernet? What are the advantages or disadvantages of one versus the other?

A. Stitched, also known as Multicard EtherSwitch, allows you to provision two or more Ethernet cards in the same chassis to act as a single Layer 2 (L2) switch. Multi-Card mode limits circuit size to STS6c, because this mode reserves the remaining STS6c of bandwidth available to the card for a stitch to other E-Series cards in the Ethergroup. This limitation does not allow you to fully utilize your bandwidth. However, all installed Ethernet cards in an Ethergroup can transmit to and receive from any provisioned Ethernet circuit and VLAN(s). The most common application for this mode of operation is the use of Shared Packet Rings, which utilize Spanning Tree Protocol rather than SONET switching to provide redundancy. This makes more efficient use of SONET bandwidth as the circuits are created unprotected.

Unstitched, also known as a Singlecard EtherSwitch, allows each Ethernet card to remain a single switching entity. Unstitched circuits alleviate the limitation of STS-6. They allow the user to setup a point-to-point connection directly between two Ethernet cards on two nodes. This allows a full STS-12c to be provisioned to the card. However, the unstitched Ethernet card cannot share VLANs that are provisioned on other Ethernet cards in the node.

IP Routing and Static Routes

Q. When are static routes required on Cisco ONS 15454 network elements (NEs) in the network configuration?

A. To achieve Cisco Transport Controller (CTC) connectivity, interconnected Cisco ONS 15454 NEs use the SONET Data Communications Channel (SDCC) for communication. Communication is accomplished through a combination of the Open Shortest Path First (OSPF) routing protocol and manually-entered static routes. Static routes are required to be added in the Cisco ONS 15454 for specific IP network scenarios.

For more information, refer to Chapter 11: IP Networking of the Cisco ONS 15454 Reference Manual, Release 5.0.

See the examples given in user manuals. To add static routes, if required, go to the CTC Node view, and select **Provisioning > Network > Static Route Create**.

Q. After I have added a new Cisco ONS 15454 node to my ring, some of the nodes appear gray and display their IP address. I am not able to log into them. What causes this problem?

A. The three most common causes of this problem are explained here:

1. If two or more computers are directly connected to different nodes that belong to the same subnet, you need to add static routes on the gateway Cisco ONS 15454 nodes (where the computers connect), based on this rule:

- ◇ **Dest:** Local PC IP address Mask:255.255.255.255
- ◇ **Next Hop:** Gateway 454 IPaddress
- ◇ **Cost:** 1

This situation can arise when you already have a PC connected on the Network Management Card (NMC), and another computer directly connected to the new node is attached. In software versions 2.2.x, Proxy Address Resolution Protocol (ARP) is used for inter-nodal communication. If there is more than one node that tries to Proxy for the network, there can be contention in the network for Proxy, which can cause a shift in the IP routing among the nodes in the network. This breaks the existing IP connection. For more details, refer to the scenarios in the Cisco ONS 15454 Reference Manual, Release 5.0.

2. The new node:

- a. Has a username and password setting that is different from the other nodes.
- b. Is on a different software release.
- c. Has no DCC connectivity or has a lack of IP connectivity.

For further details, refer to 1.8.6 Node Icon is Gray in Network View of the Cisco ONS 15454 Troubleshooting Guide, Release 5.0.

3. You run a software version on your new node that is different from the version on the others. In SONET Data Communications Channel (SDCC) domains that run multiple software versions, you must always log in to the node running the latest software version to ensure backward compatibility.

Power Supply

Q. Why does a loss of DC power on the A or B inputs not generate an alarm?

A. This feature is supported in release 4.1 and later versions, when you use TCC2 cards.

Q. What are the power requirements for the Cisco ONS 15454 MSPP?

A. The power requirements for the Cisco ONS 15454 are:

- ◆ Input power: 48 Volts DC (VDC) (–42 to –57 VDC), with a maximum draw for a fully populated shelf to be 24 amps at 1016.8 watts that consume 3469.46 BTU per hour.

Q. What are the maximum Basic Transmission Units (BTUs) per hour rating for the Cisco ONS 15454?

A. In a fully populated Cisco ONS 15454 shelf (slots 1 through 17), when all cards pull the maximum load of 1016.8 watts, the Cisco ONS 15454 has a maximum BTU per hour rating of 3469.46=.

Protection Groups

Q. Can the four ports on the Optical Carrier–3 (OC–3) card be setup in a protection group? Can the ports be used for Data Communications Channel (DCC) connectivity?

A. OC–3 ports can either remain unprotected, or they can be members of a protection group. Protection is provided on a port-by-port basis, so on a single card, some ports can carry unprotected traffic, while others are members of protection groups.

Sometimes, protection groups are not created with a single card (port 1 on card A cannot protect port 2 on card A). Protection groups must be created through identical ports on two separate OC-3 cards. For example, port 1 on card A can protect port 1 on card B, but not port 2, 3, or 4 on card B. One OC-3 card can support as many as four protection groups.

This example best illustrates OC-3 protection groups:

Cards A and B are OC-3 cards that currently have no protection groups on them. A protection group is created through port 1 on card A as the protection port, and port 1 on card B as the working port. The remaining three ports on card A can remain unprotected and carry unprotected traffic. They can also serve as protection ports for working traffic carried on the three remaining ports on card B. It is possible that the remaining three ports on card A are not used for either working or protect traffic in conjunction with a third OC-3 card.

Similarly, the remaining three ports on card B can remain unprotected and carry unprotected traffic. They can also serve as working ports in protection groups, where protection traffic is carried on the three remaining ports on card A. It is possible that the remaining three ports on card B are not used for either working or protecting traffic in conjunction with a third OC-3 card.

Only ports 1 and 3 on an OC-3 card can be used for DCC connectivity. The SONET DCC (SDCC) tab allows the user to select ports 2 and 4, but this Java error appears to indicate that these are invalid choices:

```
cerent.cms.idl.SonetTopology.xInvalidDcc
```

This limitation is resolved in Release 3.0 and later, in which SDCCs are supported on all four ports of an OC3-4 card.

Provisioning

Q. Why can I not create a circuit from a DS3 card to a DS3-XM card?

A. These cards handle the SONET payloads differently (the C2 byte in the System Overhead (SOH)). A DS3 card has an asynchronous payload with a C2 hex value of 04, whereas a DS3-XM card has a Virtual Tributary (VT) payload with a C2 hex value of 02.

Q. I encounter bit errors under the Performance Monitoring (PM) tab on my optical or electrical card. What do these errors mean?

A. Bit errors on optical cards are usually a result of power levels outside the specified threshold for the OCn card in question. Low signals can be the result of poorly seated or dirty fiber connectors. They can also be caused by incorrect OCn card type in that the power budget for the particular card type is insufficient for the loss on the span. Hot signals must be attenuated such that the level is comfortably within the Rx threshold for the specified card.

Bit errors on electrical cards are generally caused by defective cabling, improperly provisioned Line Build Out, synchronization problems and defective hardware. Perform facility and terminal loopbacks to isolate the cause. Always use a test set whenever possible, because the cause of the errors could be external cabling or equipment connected to the Cisco ONS 15454.

Q. Can the Cisco ONS 15454 support STM-1?

A. Yes, you can provision the OC-3 IR 1310 card to support Synchronous Transport Module (STM)-1 signals. However all four ports on the card must be provisioned for STM-1. All four ports drop and insert STM-1 traffic in unprotected or 1+1 protected Automatic Protection Switch (APS) mode. Each STM-1 is mapped as a 155 Mbps concatenated signal (Synchronous Transport Signal (STS)-3c) for transparent transport over a SONET network. The original STM-1 traffic can be handed off as an STM-1 or an OC-3.

Q. What causes my circuits to show up as incomplete?

A. When a circuit is reported as incomplete, it does not necessarily mean that traffic is affected.

All provisioned circuits use the MAC address of a Cisco ONS 15454 to identify the source and destination endpoints of a circuit. A circuit shows up as incomplete if the MAC address of either the source node or the destination node is invalid. In the Cisco Transport Controller (CTC), check for any invalid MAC address alarms.

Furthermore, all circuit information is propagated around the network by the SONET Data Communication Channels (SDCCs) between each Cisco ONS 15454. If the Cisco ONS 15454 has not been able to obtain updated circuit information from the other nodes, circuits can show up as incomplete. In CTC, make sure that all nodes are both visible and initialized on the network map. Also, make sure that SDCC is up and running between nodes, and that you do not receive any SDCC termination failure alarms.

Q. Is the Alarm Interface Controller (AIC) card required for system operation?

A. No. The AIC card is an optional card that expands system management capabilities for customer-defined alarm I/O and orderwire. For more information on the functionality of the card, refer to Chapter 2 (Card Reference) in the Cisco ONS 15454 Reference Manual, Release 5.0.

Q. What are the node limitations for each of the ring topologies of Cisco ONS 15454?

A. From Release 3.0 onwards, the Cisco ONS 15454 supports two Bidirectional Line Switched Rings (BLSRs) with up to 16 ONS 15454 nodes. Support for up to 32 Nodes is introduced in Release 3.4, although switch times can be longer than the industry standard 60msec. For Unidirectional Path Switched Ring (UPSR) networks, the number of nodes is theoretically unlimited, but a practical limit would be 50.

Q. When I insert a Timing Control Card (TCC) into the Cisco ONS 15454 shelf, why do the Fail and Standby/Active LEDs flash continuously?

A. When a TCC is inserted in the Cisco ONS 15454 shelf, the red Fail LED flashes for several minutes. This is the normal TCC boot process.

However, sometimes the second TCC that is inserted in the Cisco ONS 15454 shelf continuously flashes the Fail and Standby/Active LEDs. This indicates that the TCC carries a different working software load compared to the active TCC in the 15454 shelf. The active

TCC is in the process of downloading its working software to the newly-inserted TCC. The active TCC always downloads its working software to the standby TCC. This process normally takes between 15 and 20 minutes. However, newer software releases can take as long as 45 minutes for the active TCC to copy the software to the standby TCC.

Q. Can a Cisco ONS 15454 network element (NE) or a network of ONS 15454 NEs have a mixture of Timing Control Card (TCC) and TCC+ cards?

A. You cannot have TCC+ and TCC cards in the same NE, but you can have TCC+ and TCC cards running in the same network.

Timing

Q. What causes timing reference switches? In other words, when is a timing reference disqualified?

A. Timing reference switches can be caused by these factors:

- ◆ The optical or Building Integrated Timing Supply (BITS) input experiences Loss of Signal (LOS) alarms, Loss of Frame (LOF) alarms, Alarm Indication Signal (AIS) alarms, or the interface is out of service.
- ◆ The Synchronous Status Messaging (SSM) indicates Do Not Use for Synchronization (DUS) alarms, or the SSM indicates that the clock is of Stratum-3 (ST-3) or lower quality.
- ◆ The input frequency is off by more than 10 ppms.
- ◆ The input clock is unstable (wandering).
- ◆ The reference has not been valid for at least two minutes.

Q. Can I daisy-chain my BITS timing source from one shelf to another?

A. No. This is an inappropriate use of the BITS interfaces, and is not supported. When you daisy-chain BITS, unnecessary wander buildup is caused in the clock network. Instead of daisy-chain, use a Timing Signal Generator (TSG) to create multiple copies of the Central Office (CO) BITS clock. Run the copies to each Cisco ONS 15454 separately.

Q. Can I time another network element (NE) from a Cisco ONS 15454 DS1 signal?

A. No. Only BITS output to another NE through the backplane pins is supported. Timing from a DS1 signal is not supported.

Q. Can I time a Cisco ONS 15454 from a DS1 that was transported through another SONET network?

A. No. This function is not supported because there is no stable clock source.

Q. How many Cisco ONS 15454 network elements (NEs) can be line-timed from another NE that derives its timing from a Stratum-1 (ST-1) BITS clock?

A. Although in theory there is no limit on the number of NEs that can be line-timed from another NE that derives its timing from a ST-1 BITS clock, a practical limit would be five hops in any one direction from the source.

Q. What are the specifications for the holdover synchronization mode in the Cisco ONS 15454?

A. A receiver clock enters holdover mode when it loses all its timing references for a significant period. The main contributors to holdover performance are:

- ◆ Initial frequency offset
- ◆ Frequency drift
- ◆ Fractional frequency offset due to temperature variations

According to GR-253 recommendation, the values must be better than these:

- ◆ Initial frequency offset less than 0.05 ppm
- ◆ Frequency drift less than 5.8×10^{-6} ppm per second
- ◆ Fractional frequency offset due to temperature variations less than 4.1 ppm

The summary of those three must be less than 4.6 ppm per day in first 24 hours of holdover mode. Technical specification for the Cisco ONS 15454 is even better than requested in the GR-253 recommendation, as shown here:

- ◆ Holdover stability, including temperature variation frequency offset, is 3.7 ppm per day.
- ◆ It results in less than 255 slips in first 24 hours of holdover mode.

Transaction Language 1 (TL1)

Q. How many simultaneous TL1 sessions can the Cisco ONS 15454 support?

A. In Release 2, ONS 15454 supports a maximum of six simultaneous TL1 sessions (five by way of the LAN port, and one by way of the serial RS-232 port).

In Release 3.0, ONS 15454 supports a maximum of 11 simultaneous TL1 sessions (10 by way of the LAN port and one by way of the serial RS-232 port).

In release 3.1 and later, 20 concurrent TL1 sessions are supported (19 by way of the LAN port and one by way of serial RS-232 port).

Q. How can I communicate with the Cisco ONS 15454 through Transaction Language 1 (TL1) commands?

A. These three options help you to communicate with the Cisco ONS 15454 through TL1:

1. Cisco Transport Controller (CTC) (GUI interface)
2. Telnet session
3. The serial RS-232 port

The maximum number of simultaneous TL1 sessions that the Cisco ONS 15454 supports depends on which software release the node runs. To determine the maximum number, refer to the How many simultaneous TL1 sessions can the Cisco ONS 15454 support? section of this document. Each TL1 option mentioned above is described in detail here:

TL1 on the Cisco ONS 15454 by way of the CTC (GUI interface)

Complete these steps in order to issue TL1 commands by way of the CTC (GUI Interface):

1. Open a browser (Netscape or Internet Explorer), and type the address of the node where you want to run TL1 commands.
2. Log in at the CTC window. The IP address at the title bar must match the IP address of the node where you want to run TL1 commands.
3. When you are logged in, click **File** located on the upper left-hand corner, then scroll to and click **TL1**.

A TL1 interface window is displayed. It has three sub-windows labeled Request History, Message Log, and TL1 Request.

You must type your TL1 commands in the last window labeled TL1 Request. The TL1 responses appear in the middle window labeled Message Log. In the top window, Request History, you can click on previous commands to recall them. When they are copied to the TL1 request line, you can press ENTER to execute that command.

4. Ensure that the **Connect** button is selected or pressed in. When it is selected, the word Connect is grayed out.
5. In the TL1 request window, issue the **ACT::USERID::PASSWORD;** TL1 command to log in, then press ENTER.

Note: You must press the ENTER key after the semicolon in each TL1 command, otherwise the commands are not executed.

6. You can also issue the **ALW-MSG-ALL;** command and press ENTER to view all TL1 messages, including unsolicited responses (for example, autonomous alarms and report events).

Note: This is also the default.

7. If you want to go back to only see messages sent in response to your commands, you can issue the **INH-MSG-ALL;** command and press ENTER.
8. You have two options to log out.

- a. Issue the **CANC-USER;** TL1 command and press ENTER.
- b. Press the **Disconnect** button.

Note: This does not close the window.

TL1 on the Cisco ONS 15454 by way of a Telnet Session

Complete these steps to issue TL1 commands by way of a Telnet session:

1. Click **Start > Run**.
2. Type **cmd** command, and click **OK**.
3. At the DOS command prompt, issue the **telnet aa.bb.cc.dd 2361** command and press ENTER, where *aa.bb.cc.dd* is the IP address of the 454 node where you want to run TL1 commands. 2361, 3082, and 3083 are the TCP ports where TL1 commands are understood. If the connection is good, a screen opens with a > prompt.
4. Issue the **ACT-USER** TL1 command to log in, as shown here:

```
>ACT-USER : : USERID : : : PASSWORD ;
```

Note: When a semicolon is typed, the TL1 command is executed immediately.

- If you do not see the characters that you type, continue with these steps:
5. Click **Terminal**, and make sure that the box Local Echo check box is checked and emulation is set to VT100.
 6. Click **OK**.
 7. Press the ENTER key. The > prompt is displayed.
 8. At the > prompt, issue the **ACT-USER** command to log in.
 9. When you log in, you see a COMPLD message.
 10. You can also issue the **>ALW-MSG-ALL;** command to see all autonomous messages sent by the node. If you want to disable or turn off the autonomous messages sent by the node, issue the **>INH-MSG-ALL;**command.

You are now able to see only the responses to the commands that you type.

11. To log out, issue the **>CANC-USER;** command.

TL1 on the 15454 with the Serial RS-232 Port

You can log into the Cisco ONS 15454 and issue TL1 commands through the serial RS-232 port located on the front of the Timing Control Card (TCC) card (slot 7 or 11).

Note: You must connect the serial cable to the active TCC.

For RS-232 connection, configure your terminal emulation software (that is, Hyperterminal) as shown here:

- ◆ Terminal emulation=vt100
- ◆ Bits per second=9600
- ◆ Data bits=8
- ◆ Parity=None
- ◆ Stop bits=1
- ◆ Flow control=None

Note: The RS-232 port located on the front of the TCC card is a DTE port.

When your emulation software is configured as described above, and your PC serial port is physically connected to the RS-232 craft port, complete these steps to issue T1 commands:

1. Press ENTER. You must see a > prompt.
2. At the > prompt, issue the **>ACT-USER::USERID:::PASSWORD;** TL1 command to log in.

Note: When a semicolon is typed, the TL1 command is executed immediately.

If you use Hyperterminal, and do not see the characters that you type, continue with these steps:

3. Click **File > Properties > Settings**.
4. Click **ASCII setup**.
5. Ensure that the Echo Typed Characters Locally check box is checked, and click **OK**.
6. Click **Emulation** and select **VT100**.
7. Click **OK**.
8. Press ENTER. You must see the > prompt. Issue a TL1 command, and you must see your characters echoed on the screen.

You can also issue the **>ALW-MSG-ALL;** command to see all autonomous messages sent by the node.

9. If you want to disable or turn off the autonomous messages sent by the node, issue the **>INH-MSG-ALL;** command.

You are now able to see only the responses to the commands that you issue.
10. To log out, issue the >CANC–USER; TL1 command.

VPN

Q. I have a VPN connection to my LAN, and I am unable to keep connectivity to the network elements (NEs). Why?

A. The problem occurs because Common Object Request Brokerage Architecture (CORBA) attempts to make a socket connection to the wrong IP address. When the Cisco ONS 15454 receives a packet from a PC, it sees the IP address of the PC, but the address that is published on the tunnel (Internet) is the address for the VPN. The Cisco ONS 15454 attempts to respond to the IP address of the VPN. The router does not recognize this address and in turn, drops the packet, which causes Cisco Transport Control (CTC) to temporarily timeout. There is approximately a 20-second timeout for the CTC session on the PC. When CTC loses the connection to the PC, the PC re-establishes the connection. The CTC cycles in and out indefinitely as the PC and the node try to communicate with one another.

From Release 3.3 onwards, CTC can communicate with an NE over VPN if the these statements are true:

- ◆ The gateway NE (GNE) proxy mode is enabled.
- ◆ The GNE can open a backward connection to the CTC host.
- ◆ Any Network Address Translation (NAT) between the CTC host and the GNE is bi-directional.
- ◆ There is no Port Address Translation (PAT) between the CTC host and the GNE (BTW, PAT is what boxes such as LinkSys use).

From Release. 4.0 onwards, all but the first item from the list above, are no longer restrictions. In Release. 4.0, only port 80 and 1080 are required.

Simple Network Management Protocol (SNMP)

Q. Does the Cisco ONS 15454 support SNMP?

A. Yes, the Cisco ONS 15454 supports SNMPv1 and SNMPv2c. It also allows some SNMP set commands.

Q. How can I setup SNMP with the Cisco ONS 15454?

A. For information on how to set up SNMP, refer to Chapter 4: Turn Up Node of the Cisco ONS 15454 Procedure Guide, Release 5.0.

Q. What is the maximum number of SNMP trap destination that can be configured in the Cisco ONS 15454?

A. A maximum of ten SNMP trap destinations can be configured in the Cisco ONS 15454.

Q. Where can I find the Cisco ONS 15454 Management Information Bases (MIBS)?

A. MIBS can be found on the distribution CD for the software and documentation. You can also download MIBS from Cisco.com with a valid CCO account.

Q. Can I use SNMP with my firewall?

A. Yes, release 4.6 software supports this feature.

Q. Does Cisco ONS 15454 SNMP support Remote Monitoring (RMON)?

A. Yes, refer to Chapter 8: Monitor Performance of the Cisco ONS 15454 Procedure Guide, Release 5.0 for more information.

Q. Can I use CiscoWorks to manage my Cisco ONS 15454?

A. No. Even though CiscoWorks is an SNMP manager, it does not have ONS 15454 MIBS pre-compiled. CiscoWorks only support IOS-based systems.

Q. Can I use network manager supplied by any vendor to send and receive SNMP traps from the Cisco ONS 15454?

A. Yes, but the network manager must allow you to load and compile MIBS. You can find the procedure to load and compile ONS 15454 MIBS in Cisco ONS 15454 Reference Manual, Release 5.0.

Related Information

- [Optical Technology Support Pages](#)
- [Cisco ONS 15454 Documentation](#)
- [Clearing DS3XM Clearing DS3XM Alarm Indication Signal-Virtual Tributary Alarms](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 02, 2006

Document ID: 46249
