Cisco Carrier Packet Transport Release Notes

The Cisco Carrier Packet Transport (CPT) Release notes contains the enhancements for the CPT platform. For detailed information regarding features, capabilities, hardware, and software introduced with this release, see *Cisco CPT Configuration Guide*. For the latest version of the Release Notes for the Cisco Carrier Packet Transport, visit the following URL:

http://www.cisco.com/en/US/products/ps11348/prod_release_notes_list.html

Note The terms "Cisco CPT" and "CPT" are used interchangeably.

Cisco also provides Bug Toolkit, a web resource for tracking defects. To access Bug Toolkit, visit the following URL:

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

This chapter includes the following topics:

Upgrading to Release 9.5.3

Critical Bug Fixes

It is recommended to use Release 9.5.3 that is the latest release of Cisco CPT.

Release 9.5.3 addresses the following critical fixes:

- **CSCug79489**: After an upgrade from 9.5.1 to 9.5.2.1, the CPT 50 card did not come up.

- **CSCuh32113**: When TNC was activated after the system upgrade from 9.5.2 to 9.5.3, TNC rebooted continuously and could not be recovered.
- **CSCui67091**: After an upgrade from 9.5.2 to 9.5.3, state of all the MPLS-TP tunnels and pseudowires were changed to PARTIAL.
- **CSCui37663**:After an upgrade from 9.5.2.3 to 9.5.3, the SAT-COMM-FAIL alarm was observed.
- **CSCug91371**: An upgrade to 9.5.1.3 failed because the active PTF card failed in between the upgrade process.
- **CSCue38018**: After an upgrade from 9.5.1.2 to 9.5.2, database loss occurred if EVC was created on the same interface as that of pseudowire AC endpoints.
- **CSCub41943**: During the upgrade from 9.5.0 to 9.5.1, Transport Node Controller (TNC) card crashed when the channel-group data was fetched.
- **CSCug47083**: After an upgrade from 9.5.1 to 9.5.2.1, the EVPL circuits stopped forwarding traffic.
- **CSCug29140**: A pseudowire with a name containing a space at the beginning and the end disappeared when the CPT system was upgraded from 9.5.2.1 to 9.5.3.
- **CSCuh15144**: After an upgrade from 9.5.1 to 9.5.2.1, the SAT-COM-FAIL alarm was observed with the severity as minor.
- **CSCud90557**: Database loss occurred when the user performed the following steps:
  - Created an MPLS-TP link with the IP address that was assigned to a port.
  - Deleted that IP address.
  - Reset the card.
- **CSCui04191**: Database loss occurred when the user performed the following steps:
  - Configured a Link Aggregation Group (LAG).
  - Configured a pseudowire over this LAG.
  - Changed the MTU value of the LAG to less than the MTU value of the pseudowire.
  - Reset the card.
- **CSCui62283**: Database loss occurred when the user performed the following steps:
  - Configured a Link Aggregation Group (LAG).
  - Configured a pseudowire over this LAG with default MTU.
  - Changed the MTU value of the pseudowire to more than the MTU value of the LAG.
  - Reset the card.
- **CSCui50716**: Database loss occurred when the user performed the following steps:
  - Configured a Link Aggregation Group (LAG).
  - Configured a pseudowire over this LAG with MTU value more than the MTU value of the LAG .
  - Reset the card.

- **CSCui22484**: Database loss occurred when the user performed the following steps:
  - Configured a pseudowire.
  - Changed the MTU value of the pseudowire.
  - Changed the MTU value of the port to less than the MTU value of the pseudowire.
  - Reset the PTF card.
- **CSCui12072**: Database loss occurred when the user performed the following steps:
  - Created a policy-map.
  - Created another policy-map and attached previously created policy-map with it as a child policy.
  - Edited the child policy.
  - Reset the card.
- **CSCud66930**: Database loss occurred when the user performed the following steps:
  - Created a channel group using different ports.
  - Configured the ingress policy on one of the member ports.
  - Reset the card.
- **CSCuh19362**: Database loss occurred when the user performed the following steps:
  - Create a Pseudowire Class enabled with Static OAM class.
  - Deleted the Static OAM class from CTC.
  - Reset the card.
- **CSCui09652**: Database loss occurred when the pseudowire and destination port of a span were configured on the same port where a channel-group was already configured.
- **CSCuh71428**: Database loss occurred when the Pluggable Port Module (PPM) was deleted where the table-map was already configured.
- **CSCui11280**: Database loss occurred when an MPLS-TP link was configured the port which was destination port of a span.
- **CSCui58996**: Database loss occurred when the Label Distribution Protocol (LDP) was configured on the port where a Resilient Ethernet Protocol (REP) was already configured.
- **CSCui60106**: Database loss occurred when the Label Distribution Protocol (LDP) was configured on the port where an EVC was already configured.
- **CSCug92219**: The ONS-SC-E1-T1-CES and ONS-SC-E3-T3 SFPs did not work with CPT 50. The traffic did not flow and certain invalid parameters were observed during the provisioning.
- **CSCuh51631**: DS3 traffic did not resume after the PTF card was reset multiple times.
- **CSCuc84965**: The traffic was not flowing on 1 G CPT 50 when the user performed the following steps:
  - Created multiple Pluggable Port Modules (PPMs).
  - Deleted these PPMs in the reverse order of creation.

- Recreated a PPM and configured services on it.

- **CSCud70712**: Traffic flow was not observed for the static pseudowires when the following steps were performed:
  - Configured an MPLS-TP tunnel and LDP on the same link number.
  - Configured 500 static pseudowires and 436 dynamic pseudowires.
  - Shut the core ports and waited for 10 minutes.
  - Run the no shut command.

- **CSCuh29838**: Traffic flow was not observed for certain pseudowires when the following steps were performed:
  - Configured an MPLS-TP tunnel and LDP on the same link number.
  - Configured 500 static pseudowires and 436 dynamic pseudowires.
  - Shut the core ports and waited for 10 minutes.
  - Run the no shut command.

- **CSCub94383**: TNC crashed on retrieving the equipment entity parameters when the CPU usage was high.
- **CSCui45278**: PTF crashed when Connectivity Fault Management (CFM) was configured and the CPU usage was high.
- **CSCui39559**: Standby PTF card reset when more than 1532 point–to–point (P2P) EVCs with Ethernet type dot1q were created.
- **CSCuh76534**: The table-map did not synched with the PTF card when more than one table-maps were configured on the port and the table-map used with the port was not first configured table-map.
- **CSCui33079**: PTM card crashed when the policy-map configuration was changed.
- **CSCuc64508**: The hostname of the PTF card changed to an IP address after a switchover was performed.
- **CSCuf17323**: The PTF card reset on a CPT 50 port when the following tasks were performed simultaneously on the port:
  - Run the shut or the no shut commands using CPO or CTC.
  - Provisioned EVC using CPO.

- **CSCui50097**: The standby PTF card reset due to non-default label mismatch which was configured before Stateful Switchover (SSO).
- **CSCui01457**: The PTF card crashed when the following tasks were performed:
  - Configured an MPLS-TP tunnel.
  - Configured at least two VPWS circuits.
  - Configured CFM MEP on both the pseudowires.
  - Initiated both the IP SLA sessions from both the ends when the remote MEP was up.
  - Removed the IP SLA session and CFM MEP from one of the services.

- **CSCue27382**: Keepalive failures were observed at TNC when the line card was deleted using CTC. The PTF cards did not receive the boot-up response from TNC even after these were hard booted.
- **CSCtz32511**: CTC did not allow the user to create Generic Communications Channels (GCC) for GCC rates 192k and 400k.
- **CSCua75095**: CTC did not allow to delete a protected MPLS-TP tunnel if the lockout was enabled on one of its LSPs. The state of MPLS-TP tunnel changed to PARTIAL in CTC, but it remained as UP in Cisco IOS.
- **CSCug47241**: CTC did not allow to create a pseudowire between two nodes from releases 9.5.1 and 9.5.2.2 respectively.
- **CSCuh96531**: CTC allowed the user to create an EVC circuit or a pseudowire with Ethernet type dot1ad on the port where Ethernet type dot1q was already configured.
- **CSCui19292**: CTC allowed the user to enable MVR on the point–to–multipoint (P2MP) Bridge where Ethernet type dot1q was already configured.
- **CSCug65485**: When editing the policy-map using CTC QOS policy removed the policer and added it again even when no parameter was changed. This impacted services that were provisioned for the EVC.
- **CSCuh97941**: CTC displayed 0 as VLB Preempt Delay on the **Open Packet Transport View** > **Provisioning** > **REP** > **Segment** tab when a segment was created with VLB Preempt Delay enabled and with some valid preempt delay value.
- **CSCuh12243**: CTC displayed an error message when the user selected and deselected the queuing options for creating a table-map under the **Provisioning** > **QoS** > **Policy Map** > **Create Policy Map** > **Action** > **Queuing** tab.
- **CSCuf16842**: The SNMP agent was getting stuck on the CPT 600 or CPT 200 chassis. This was observed for multiple versions of SNMP.
- **CSCug18181**: A CPT 50 console did not ask for credentials when accessed from any other CPT 50 device.
- **CSCud34373**: Channel groups were not listed in the **Available Ports** drop-down list of the EFP Configuration Preview screen when creating an EVC circuit using CTC.
- **CSCug92060**: Bidirectional Fault Detection (BFD) was flapping when it was configured over the unprotected tunnel midpoints.
- **CSCua07169**: A pseudowire continued to forward the traffic even when the pseudowire state was changed to DOWN using CTC.
- **CSCua88616**: If an endpoint PW neighbor was deleted from a mesh VPLS circuit containing EFPs, the VPLS circuit moved to Partial and UP state. When the VPLS circuit was cleared and re-queried, the circuits did not merge and two VPLS circuits were observed. One was in Discovered and UP state and another was in Partial and DOWN state.
- **CSCuh69954**: Error message displayed when the following steps were performed on the EFP port with VLAN range or list multiple times:
  - Shut the port.
  - Run the no shut command.
- **CSCui12192**: Policy class actions changed to 0 after it was edited for a class-map.

- **CSCui46465**: Y.1731 Delay Measurements was not working on Xconnect where MPLS-TP Tunnel and Attachment Circuit (AC) were configured.

Best Practices in Release 9.5.3

Before upgrading to Release 9.5.3, review the following best practices. CPT 9.5.3 has been enhanced to disallow certain invalid configurations that were allowed in earlier releases. If you have these configurations in your system, it is recommended to perform required changes before upgrading to Release 9.5.3. If the system is upgraded with these invalid configurations, it may result in database loss.

Note Ensure to complete critical information checks and tasks such as retain all configuration data before upgrading to the Release 9.5.3. For more information, refer to the *Upgrading the Cisco CPT to Release 9.5.x*. It is also recommended to validate the CPT database before the upgrade. Contact Cisco TAC for more information and support on getting the database validated.

- When you configure a destination port of a span, it is recommended not to use the following ports:
  - A member port of a channel group on which a pseudowire is already configured
  - A port on which an MPLS-TP is already configured
  - A port on which a fan-out group (FOG) is already configured
- When you configure a pseudowire on a port, it is recommended to set the MTU value of that pseudowire less than the MTU value of the port.
- When you configure a pseudowire on a Link Aggregation Group (LAG), it is recommended to set the MTU value of the pseudowire less than the MTU value of the LAG.
- If an IP-based MPLS-TP link is already configured on an interface, it is recommended not to remove the IP address of that interface.
- If a pseudowire class is configured on a static OAM class, it is recommended not to delete that static OAM class.
- If Y.1731 is configured on the following services, it is recommended not to delete these services:
  - Connectivity Fault Management (CFM)
  - Pseudowire
  - Ethernet Virtual Circuit (EVC)
- It is recommended to create a pseudowire class (associated to a VPLS) with the interworking as None and the signaling protocol as LDP.
- It is recommended not to enable Ethernet Synchronization Message Channel (ESMC) on the active card that you want to shut otherwise the standby card will reboot .
- It is recommended not to configure different services with the same VLAN ID.
- It is recommended not to delete the port on which the following services are configured:
  - MPLS-TP link
  - ARP-based MPLS-TP link

- QoS table-map
- Resilient Ethernet Protocol (REP)

- It is recommended not to enable Multicast VLAN Registration (MVR) on a service whose encapsulation type is not untagged.
- It is recommended not to reset the PTF card if you have configured the ingress policy on one of the member ports of a channel-group.
- When you configure a service with the default encapsulation type, it is recommended not to use the port on which a service is already configured.
- When you configure a service, it is recommended not to use the port on which an MPLS-TP tunnel is already configured.
- When configuring Y.1731 fault management parameters, it is recommended not to use the service ID that is already used for VPLS or MPLS-TP tunnel.
- When you edit a policy-map at a child level, it is recommended to edit the corresponding parent policy-map also. Click **Edit Policy Map** >**Finish** without modifying any parameters.

After upgrading to Release 9.5.3, you might encounter the following issues. Refer to the corresponding workarounds to resolve these.

- If the PTF card reboots continuously after the upgrade, power cycle the PTF card.
- If CTC displays incorrect status for all the PTM ports of a card, perform the following steps:
  1. Shut the PTM port.
  2. Run the **no shut** command.
- If the DEF-EFM-PEER-MISSING alarm is observed after the upgrade, reset the card.
- If the Sat-Comm False alarm is observed after the upgrade, perform the following steps:
  1. Shut the port on which a FOG is configured.
  2. Run the **no shut** command.

Software and Hardware Requirements

Before you begin to install CPT, you must check if your system meets the minimum software and hardware requirements. This section describes the software and hardware requirements for CPT.

- Hardware—IBM-compatible PC with a Pentium IV or faster processor, CD-ROM drive, a minimum of 1 GB RAM, 20 GB hard disk with 250 MB of available hard drive space.
- Operating System:
  - Windows 2000 Professional, Windows XP Professional, Windows Vista, or Windows 7, Windows Server 2003 or 2008.
  - UNIX workstation with Solaris Version 9 or 10 on an UltraSPARC-III or faster processor, with a minimum of 1 GB RAM and a minimum of 250 MB of available hard drive space.

- Apple Mac OS X.

  (Use the latest patch/service pack released by the OS vendor. Check with the vendor for the latest patch/service pack.)

- Java Runtime Environment—Java Runtime Environment Version 1.6.
- Browser for PC—Internet Explorer 6.x, 7.x, 8.x. For UNIX Workstation—Mozilla 1.7. For MacOS-X PC—Safari.

To install or upgrade CPT, see the guides listed in Related Documentation, on page 9.

Using the Bug ToolKit to Search Bugs

In Cisco Carrier Packet Transport Release 9.3 and later releases, use the Bug ToolKit to view the list of outstanding and resolved bugs in a release.

This section explains how to use the Bug ToolKit to search for a specific bug or to search for all the bugs in a specific release.

Procedure

Step 1 Go to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.
You will be prompted to log into Cisco.com. After successful login, the Bug Toolkit page opens.

Step 2 To search for a specific bug, enter the bug ID in the **Search for Bug ID** field and click **Go** in the **Search Bugs** tab.
To search for bugs in a specific release, enter the following search criteria:

- Select Product Category—Select **Optical Networking**.
- Select Products—Select **Cisco Carrier Packet Transport (CPT) System** from the list.
- Software Version—Select **9.5.3** to view the list of outstanding and resolved bugs in the Cisco CPT software.
- Search for Keyword(s)—Separate search phrases with boolean expressions (AND, NOT, OR) to search within the bug title and details.
- Advanced Options—You can either perform a search using the default search criteria or define custom criteria for an advanced search. To customize the advanced search, select **Use custom settings for severity, status, and others** and provide the following information:

  - Severity—Select the severity level from 1 to 6.
  - Status—Select **Open**, **Fixed**, or **Terminated**.

    Select **Open** to view all the open bugs. To filter the open bugs, uncheck the **Open** check box and select the appropriate sub-options that appear below the Open check box. The sub-options are New, Held, More, Open, Waiting, Assigned, Forwarded, Postponed, Submitted, and Information Required. For example, if you want to view only new bugs in Cisco CPT Release 9.3, only select **New**.

Select **Fixed** to view fixed bugs. To filter fixed bugs, uncheck the **Fixed** check box and select the appropriate sub-options that appear below the Fixed check box. The sub-options are Resolved or Verified.

Select **Terminated** to view terminated bugs. To filter terminated bugs, uncheck the **Terminated** check box and select the appropriate sub-options that appear below the Terminated check box. The sub-options are Closed, Junked, and Unreproducible. Select multiple options as required.

- Advanced—Check the **Show only bugs containing bug details** check box to view only those bugs that contain detailed information, such as symptoms and workarounds.
- Modified Date—Select this option if you want to filter bugs based on the date on which the bugs were last modified.
- Results Displayed Per Page—Select the appropriate option from the list to restrict the number of results that appear per page.

Step 3 Click **Search**. The Bug Toolkit displays the list of bugs based on the specified search criteria.

Export to Spreadsheet

The Bug ToolKit provides the following options to export bugs to a spreadsheet:

- Click **Export All to Spreadsheet** link in the Search Results page under the Search Bugs tab. Specify file name and folder name to save the spreadsheet. All the bugs retrieved by the search will be exported.
- Click **Export All to Spreadsheet** link in the My Notifications tab. Specify file name and folder name to save the spreadsheet. All the saved bugs in all the groups will be exported.

If you are unable to export the spreadsheet, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1-800-553-2447).

Related Documentation

Use the Cisco CPT Release Notes, Release 9.5.3 in conjunction with the following referenced Release 9.5.3 publication:

- Cisco CPT Hardware Installation Guide
- Cisco CPT Configuration Guide
- Cisco CPT Command Reference Guide
- Upgrading the Cisco CPT to Release 9.5 and 9.5.x
- Cisco CPT Licensing Configuration Guide

Additional References

The following link provides additional information on CPT:

- http://www.cisco.com/go/cpt

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.