Cisco Carrier Packet Transport Release Notes

The Cisco Carrier Packet Transport (CPT) Release notes contain the new features and 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

Revision History

Date	Notes
March 2013	Added critical bug fixes made in Release 9.5.2.1 in the Critical Bug Fixes, on page 2 section.
January 2013	Added critical bug fixes made in Release 9.5.2 in the Critical Bug Fixes, on page 2 section.
November 2012	Added critical bug fixes made in Release 9.5.1.2 in the Critical Bug Fixes, on page 2 section.
October 2012	Added critical bug fixes made in Release 9.5.1.1 in the Critical Bug Fixes, on page 2 section.

This chapter includes the following topics:

Critical Bug Fixes

Critical Bug Fixes in Release 9.5.2.1

It is recommended to use Release 9.5.2.1 that is the latest release of Cisco CPT.

Release 9.5.2.1 addresses the following critical bug fixes over 9.5.2.

- **CSCue94077**: CTC did not allow to enter VLAN range when creating a class map.
- **CSCue73421**: When the show running-config command was executed through a telnet session for a large configuration file, the contents of the configuration file was displayed as garbled.
- **CSCue73365**: CTC and Cisco IOS allowed to configure an MPLS-TP link on the same interface on which a pseudowire, and Ethernet Virtual Circuit (EVC) was already configured. Similarly, CTC and Cisco IOS allowed to configure a pseudowire and EVC on the same interface on which an MPLS-TP lin was already configured.
- **CSCue54833**: CTC did not allow spaces in the PW Name field when creating a new pseudowire.
- **CSCue66419**: CTC did not allow the user to create a multisegment pseudowire.
- **CSCue91711**: The bandwidth value of a pseudowire changes to 0 when any modification is made on the **Edit Circuit** > **General** tab.

Critical Bug Fixes in Release 9.5.2

Release 9.5.2 addresses the following critical fixes over Release 9.5.1.2:

- **CSCtw96586**: Egress Quality of Service (QoS) was not working on point-to-multipoint (P2MP) EVC after a node power cycle.
- **CSCtx24528**: Egress QoS was not working when power cycling the node with Virtual Private LAN Services (VPLS) and a port-channel on a CPT 50 panel that was fanned out from a trib card.
- **CSCuc01160**: Traffic flow rate on Ethernet Flow Points (EFPs) dropped when an ingress QoS service policy was applied on an EFP when the encapsulation is double VLAN tagged and inner tag was VLAN range.
- **CSCtx00536**: Committed information rate (CIR) was not working for SFP+1 and SFP+2 ports in UL at the interface level.
- **CSCub23788**: ITU-T Y.1731 delay measurement was not working on a port-channel interface when the maintenance association profile was configured on a pseudowire and an EVC where the pseudowire was configured first followed by the EVC.
- **CSCub36186**: Layer 2 virtual forwarding interface (VFI) became partial when the existing endpoint psuedowire neighbor is deleted in a mesh VPLS circuit containing EFPs.

- **CSCtx05374**: High traffic switch time was observed during interconnect (IC) link switchover.
- **CSCtz80539**: Ethernet Connectivity Fault Management (CFM) UP maintenance endpoints (MEPs) did not learn the remote MEPs after 512 entries.
- **CSCud05137**: CTC always displayed the bandwidth (BW) value of an MPLS-TP tunnel as a rounded numerical value. For example, if 1500 Mbps was entered as the BW value when creating an MPLS-TP tunnel, CTC displayed it as 1 Gbps instead of 1.5 Gbps when the MPLS-TP tunnel was successfully created.
- **CSCud95214**: If unknown nodes existed in the network, CTC did not display some of the PPC spans in the route of the MPLS-TP tunnel that was displayed in the TP Tunnel Circuit Routing Constraints screen.
- **CSCto67716**: CTC displayed the default values of the optics PM parameters such as laser bias, receive optical power, and transmit optical power instead of NA on the **Performance** > **Optics PM** > **Current Values** tab for the SFPs that are not supported in CPT. These SFPs are ONS-SI-100-FX, ONS-SI-100-LX10, and ONS_SI_GE_LX.
- **CSCua91006**: CTC displayed -40dBm instead of NA in all the columns on the **Performance** > **Optics PM** > **Current Values** tab when a copper SFP was inserted into a CPT 50 slot.
- **CSCub60793**: CTC and Cisco IOS allowed Resilient Ethernet Protocol (REP) to be configured on the main port-channel interface.
- **CSCuc57227**: CTC allowed a port to be configured as a destination port when that port was a part of source port-channel in a span session.
- **CSCuc31758**: CTC allowed the interworking and protocol of a pseudowire class associated with a VPLS to be edited.
- **CSCub50449**: CTC displayed an error and did not reflect the required configuration when the following steps were performed:
  - Created a policy map.
  - Selected the set-cos-transmit and set-dcsp-transmit actions in the conform or exceed category.
- **CSCua49867**: Port state (10 GE and 1GE) of a CPT 50 panel that was displayed in CTC was different from the port state displayed in Cisco IOS.
- **CSCtz68644**: Packet Transport Fabric (PTF) card reset continuously due to a communication failure between the Transport Node Controller (TNC) and the PTF card.
- **CSCua26265**: Error burst was observed in DS1/DS3 traffic after the TNC card was reset.
- **CSCub33820**: The management connectivity of the CPT 200 or CPT 600 shelves running TNC or TSC cards was lost.
- **CSCuc81545**: Uplink card restarted continuously when a table map was applied to an interface where an MPLS-TE tunnel was created.
- **CSCty88141**: Egress span was not working on multiple cards.
- **CSCtz85679**: A memory leak was observed when configuring an EFP span for a range of EFPs that had more than eight EFPs.
- **CSCuc65212**: Database loss occurred when a port (with L2PT configuration) that was provisioned on an uplink card, a CPT 50 panel or a trib card was deleted and the uplink card was reset.

- **CSCua09563**: Database loss occurred when CTC allowed an REP link and an MPLS-TP link to be configured on the same interface.
- **CSCuc36879**: Database loss occurred when the protocol and status of a pseudowire class were modified as LDP and oam respectively.
- **CSCud53118**: Database loss occurred when a fully loaded CPT 600 chassis was upgraded from Release 9.5.1 to Release 9.5.2.
- **CSCud94948**: Database loss occurred when the following steps were performed:
  - Configured a pseudowire.
  - Changed the default MTU value of the pseudowire.
  - Changed the default MTU value of the interface. It was less than the MTU value of the pseudowire.
  - Reset the PTF Card.
- **CSCud97770**: Database loss occurred when the following steps were performed:
  - Opened a card and created a new table map on the **PTS view > Provisioning > QoS**tab.
  - Associated the table map with the port that had the Table Map Config as MPLS.
  - Deleted this table map.
  - Reset the active and standby uplink card.
- **CSCuc39477**: Database loss occurred when the following modifications were applied to a pseudowire class that was associated with VPLS and then the PTF cards were reset:
  - Selected TE over TP as the tunnel type for the preferred path.
  - Enabled BFDoVCCV.
- **CSCtq67285**: A traffic hit was experienced in the following scenarios:

  Scenario A

  - A card was associated with one Fan-Out-Group (FOG).
  - Another FOG was added to the same card.

  Scenario B

  - A card was associated with two FOGs.
  - Any one of the FOGs was deleted from the same card.

Critical Bug Fixes in Release 9.5.1.2

Release 9.5.1.2 addresses the following critical fix over Release 9.5.1.1:

- A pseudowire class could not be selected when creating a VPLS circuit using three nodes or more as the PW Class A and PW Class Z drop-down lists in the VPLS Configuration screen were disabled.

Critical Bug Fixes in Release 9.5.1.1

Release 9.5.1.1 addresses the following critical fixes over Release 9.5.1:

- CFM was not working for pseudowires with the following encapsulation type:
  - encapsulation double tagged with single outer VLAN and multiple inner VLANs
- Ethernet frame Delay Measurement (ETH-DM) in Y.1731 performance monitoring was not working for pseudowires with the following encapsulation types:
  - encapsulation untagged
  - encapsulation untagged list, range
  - encapsulation double tagged with single outer VLAN and multiple inner VLANs

Note ITU-T Y.1731 is enhanced in Release 9.5.1.1 to support untagged frames.

- Hierarchical Ingress service policy was not working for the incoming encapsulation type as encap dot1q <id> second-dot1q <range>.
- CTC allowed the BW value of MPLS-TP tunnels to be edited in the Partial state.
- CTC did not allow the MPLS-TP tunnels to be deleted in the Partial state.
- CTC did not send update events to the Cisco Prime Optical (CPO) when a channel group was created or the Port name was modified.
- TNC crashed when upgraded from version 9.5.0 to 9.5.1.
- CTC and Cisco IOS displayed invalid BW value when the following steps were performed:
  1. Created an MPLS-TP tunnel with midpoint configuration such that at least two tunnels were in the Partial state.
  2. Edited the BW value of the MPLS-TP tunnel such that the BW value exceeded the default value of 10 GB.
- Database loss occurred when the following steps were performed:
  1. Opened a card and provisioned a port on the **Provisioning** > **Pluggable Port Modules** tabs.
  2. Configured L2PT Config settings on the **Provisioning** > **Ether Ports** > **Ethernet** tabs.
  3. Deleted the port. This led to database corruption.
  4. In CPT 200 chassis, reset the uplink card.

     In CPT 600 chassis, reset both the active and standby uplink cards.

For information on other bugs fixed in this release, use the Bug ToolKit.

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.

New Features and Functionality

No new feature or functionality is added in Releases 9.5.1.1, 9.5.1.2, 9.5.2, and 9.5.2.1. This section highlights new features and functionality for Release 9.5.1. For detailed documentation for the configuration as well as limitations of each of these features, see the Cisco CPT Configuration Guide.

Software

The CPT Release 9.5.1 supports the following software features.

Y.1731 Fault Management and Performance Monitoring

Y.1731 is an extension of the Connectivity Fault Management (CFM). The ITU-T Y.1731 feature provides operations, administration, and maintenance (OAM) functions for fault management and performance monitoring to serve the needs of service providers in a large network.

CPT supports Ethernet Alarm Indication Signal (ETH-AIS), Ethernet Remote Defect Indication (ETH-RDI), and Ethernet Locked Signal (ETH-LCK) functionality for fault detection and isolation.

Y.1731 Performance Monitoring (PM) provides a standard Ethernet PM function that includes measurement of Ethernet frame delay, frame delay variation, frame loss, and frame throughput measurements specified by the ITU-T Y-1731 standard. To measure Service Level Agreement (SLA) parameters such as frame delay or frame delay variation, a small number of synthetic frames are transmitted along with the service to the maintenance end point (MEP).

CPT supports only two–way Ethernet frame Delay Measurement (ETH-DM) in Y.1731 performance monitoring. The CPT system sends, receives, and processes PM frames in intervals of 100 ms (10 frames per second) and 1 second.

Note CFM must be enabled in the network for Y.1731 to become operational.

Span

Span is a technique of replicating the ingress or egress frames in a specific port to a specified list of destination ports. It is a monitoring feature used to monitor the traffic that is coming in and out of a port, channel group, or an Ethernet Flow Point (EFP). The monitored traffic can be used to debug the network and can also be used by law enforcement agencies.

The span can be configured to monitor ingress traffic, egress traffic, or both. The span source can be a physical port, channel group, or an EFP. The span destination can be a physical port or a channel group.

CPT supports two span modes:

- Port Span—In this configuration, the ingress or egress traffic on all the Ethernet Virtual Circuits (EVCs) in the source port or channel group is captured on the destination port or channel group. The pseudowire or tunnel port is not supported as a span destination.
- EFP Span—In this configuration, the ingress or egress traffic on the specified EFPs on a particular port or channel group is captured on the destination port or channel group. All types of services such as Multiprotocol Label Switching (MPLS), Virtual Private LAN Service (VPLS), Virtual Private Wire Service (VPWS), xconnect can be monitored. The pseudowire or tunnel port is not supported as a span destination.

Interlink QoS

Traffic from 1 GE ports of CPT 50 to CPT 200 or CPT 600 can be prioritized when there is congestion on the 10 GE interlink ports. CPT provides strict priority queuing mode. In this mode, the qos-group 7 and qos-group 3 share the same and highest priority than the remaining six queues. These two queues are scheduled on a round-robin basis if there is traffic on both these queues. The remaining six queues are configured in strict priority scheduling mode in the following order: Qos-group 6, 5, 4, 2, 1, 0.

Support for MSTP Cards

The following MSTP cards are supported in the CPT 200 and CPT 600 chassis:

- 15454-40-SMR2-C=
- 15454-40-SMR1-C=
- 15454-AR-XP=
- 15454-AR-XP-LIC=
- 15454-AR-MXP=
- 15454-AR-MXP-LIC=
- 15454-OTU2-XP=
- 15454-ADM-10G=

- 15454-OPT-AMP-17C=
- 15454-OPT-AMP-C=
- 15216-MD-40-ODD=
- 15216-MD-40-EVEN=
- 15216-FLD-4-30.3=
- 15216-FLD-4-33.4=
- 15216-FLD-4-36.6=
- 15216-FLD-4-39.7=
- 15216-FLD-4-42.9=
- 15216-FLD-4-46.1=
- 15216-FLD-4-49.3=
- 15216-FLD-4-52.5=
- 15216-FLD-4-55.7=
- 15216-FLD-4-58.9=

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 **9.30**, **9.301**, **9.302**, **9.5.0**, **9.5.1**, **9.5.1.1**, **9.5.1.2**, **9.5.2**, or **9.5.2.1** 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.x in conjunction with the following referenced Release 9.5.x 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.