Release Notes for Cisco CPT–CTC and Documentation Release 9.5 and Cisco IOS Release 15.2(01)SA

Revised: February 1, 2012, OL-26263-01

Cisco Carrier Packet Transport Release Notes

The Cisco Carrier Packet Transport (CPT) 9.5 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–CTC and Documentation Release 9.5 and Cisco IOS Release 15.2(01)SA*. For the latest version of the Release Notes for Carrier Packet Transport Release 9.5, visit the following URL:

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

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

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 6.

New Features and Functionality

This section highlights new features and functionality for Release 9.5. For detailed documentation of each of these features, see the *Cisco CPT Configuration Guide–CTC and Documentation Release 9.5 and Cisco IOS Release 15.2(01)SA*.

Hardware

The CPT Release 9.5 supports the following hardware:

SFP Support

The following SFPs are supported in CPT:

- ONS-SC+-10G-ZR=, ONS-SC+-10G-LRM=, ONS-SC+-10G-xx.x= (xx.x = 30.33 to 60.61, 40 DWDM wavelengths), ONS-SE+-10G-LR= on Cisco CPT 200, Cisco CPT 600, and 10 GE ports of Cisco CPT 50.
- ONS-SC+-10G-ZR=, ONS-SC+-10G-LRM=, ONS-SC+-10G-xx.x= (xx.x =), ONS-SC-E1-T1-CES=, ONS-SC-E3-T3-CES=, ONS-SC-2G-xx.x= (xx.x = 30.33 to 60.61), ONS-SC-GE-BXU=, ONS-SC-GE-BXD=, ONS-SI-GE-EX= on 1 GE ports of Cisco CPT 50.

Software

The CPT Release 9.5 supports the following software features. You can configure the software features either through CTC or Cisco IOS commands.

Virtual Private LAN Service

Virtual Private LAN Service (VPLS) is a multipoint Layer 2 VPN technology, which allows multiple sites to be connected over a simulated Ethernet broadcast domain that is supported across a provider provisioned IP/MPLS network. In other words, VPLS delivers multipoint Layer 2 connectivity over a Layer 3 network architecture. VPLS evolved as a logical extension of Ethernet over MPLS (EoMPLS), which was developed to enable point-to-point Ethernet-based Layer 2 VPN services.

Connectivity Fault Management

Connectivity Fault Management (CFM) is an end-to-end per-service Ethernet layer OAM protocol. End-to-end CFM can be provider edge to provider edge (PE to PE) or customer edge to customer edge (CE to CE). CFM includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs. CFM is defined in the IEEE 802.1ag standard.

Troubleshooting carrier networks offering Ethernet Layer 2 services is challenging. Customers contract with service providers for end-to-end Ethernet service and service providers may subcontract with operators to provide equipment and networks. These networks belonging to distinct organizations or departments are substantially larger and more complex and have a wider user base. CFM provides a competitive advantage to service providers where the operational management of link uptime and timeliness in isolating and responding to failures is crucial to daily operations.

CPT supports the IEEE standard implementation of CFM. It supports CFM over point–to–multipoint bridge domain associated with an Ethernet Flow Point (EFP), Xconnect, and port Maintenance End Point (MEP).

Ethernet Link OAM

Ethernet link Operation, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet MANs and Ethernet WANs. Ethernet link OAM is defined in the IEEE 802.3ah standard.

The Ethernet Link OAM protocol enables service providers to monitor and troubleshoot a single physical (or emulated) Ethernet link. It supports link level verification, monitoring, and troubleshooting between two Ethernet devices.

Synchronous Ethernet

A separate external time-division multiplexing (TDM) circuit is required to provide synchronized timing to multiple remote network elements (NEs) for packet transport networks like CPT. The Synchronous Ethernet (SycnE) feature addresses this requirement by providing effective timing to the remote NEs through a packet network without using an external circuit for timing.

With Ethernet equipment gradually replacing existing Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) equipment in service provider networks, frequency synchronization is required to provide high-quality clock synchronization over Ethernet ports. The SyncE feature provides the required synchronization at the physical level. Operation messages maintain SyncE links and ensure that a node always derives timing from the most reliable source. SyncE uses the Ethernet Synchronization Message Channel (ESMC) to enable traceability of the best clock source to correctly define the timing source and prevent a timing

loop. Besides ESMC, CPT also uses the Synchronization Status Messaging (SSM) for time synchronization using Optical Transport Network (OTN) ports.

Match VLAN for QoS

The capability to classify the traffic based on the outer VLAN ID is introduced in quality of service (QoS). The **match-all** keyword is added to the **match** command to have a capability to match all the classification criteria present in the QoS class-map.

Remote Ethernet Port Shutdown

The Remote Ethernet Port Shutdown feature allows a service provider edge router on the local end of an EoMPLS pseudowire to detect a remote link failure and cause the shutdown of the Ethernet port on the local customer edge router. Shutting down the Ethernet port on the local customer edge router prevents or mitigates a condition where that router would otherwise lose data by forwarding traffic continuously to the remote failed link, especially if the link was configured as a static IP route.

In-Service Software Upgrade Enhancement

The In-Service Software Upgrade (ISSU) message transformations between the active fabric card and the line card is supported. All the CPT components support the ISSU message transformations between the active fabric card and the line card except the Ethernet Virtual Circuit (EVC) and QoS components.

Bandwidth Management

Bandwidth can now be specified for an Multiprotocol Label Switching Transport Profile – Traffic Engineering (MPLS-TE) tunnel, Multiprotocol Label Switching – Transport Profile (MPLS-TP) tunnel, and a pseudowire. This bandwidth is checked against the available bandwidth. If the specified bandwidth exceeds the available bandwidth, the service cannot be created.

The specified bandwidth is used only for accounting purposes. The specified bandwidth is not reserved by the CPT system for the actual traffic. The bandwidth value is not enforced on the services.

MIB Support

The following Management Information Base (MIBs) are newly supported in CPT 9.5:

- CISCO-DOT3-OAM-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-EVC-MIB
- DS1-MIB.my
- DS3-MIB.my
- ETHERLIKE-MIB
- IEEE8021-CFM-MIB
- IF-MIB
- MPLS-LDP-STD-MIB
- MPLS-LSR-MIB.my
- MPLS-LSR-STD-MIB.my
- RMON-MIB-V1SMI/HC-RMON-MIB
- SNMPV2-MIB

For more information on supported MIBs in CPT, see the SNMP chapter of *Cisco CPT Configuration Guide*.

Node Addition

A MPLS–TP tunnel can traverse through multiple nodes. The Node Addition feature is a CTC enhancement that allows new nodes to be added over an existing MPLS–TP tunnel. If a new node needs be added to the network, the MPLS–TP tunnel need not be deleted or rerouted. Instead, CTC will rediscover the path and re-direct the MPLS–TP tunnels.

Commands Not Supported

The **copy** and **boot system** Cisco IOS commands are not supported in CPT.

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**, or **9.50** 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 in conjunction with the following referenced Release 9.5 publication:

- *Cisco CPT Hardware Installation Guide*
- *Cisco CPT Configuration Guide-CTC and Documentation Release 9.5 and Cisco IOS Release 15.2(01)SA*
- *Cisco CPT Command Reference Guide-CTC and Documentation Release 9.5 and Cisco IOS Release 15.2(01)SA*
- *Upgrading the Cisco CPT to Release 9.5*
- *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 an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS version 2.0.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands