

Juniper Networks® CTPOS 6.0 Software Release Notes

Release 6.0R1
June 2010
Revision 1

These release notes accompany Release 6.0R1 of the CTPOS software. They describe device documentation and known problems with the software.

You can also find these release notes on the Juniper Networks CTP software documentation Web page, which is located at

http://www.juniper.net/techpubs/en_US/release-independent/ctp/information-products/pathway-pages/index.html.

Contents

Upgrade Notes	3
New Features	3
CTP150 Hardware Platform	3
Interoperability with M Series E1/T1 Circuit Emulation PICs Using SAToP Bundles	3
Hot-Swap Interface Module Replacement on CTP2000 Devices	4
Route Management Redundancy is Now Link State Aware	5
CESoPSN Bundles Now Support BERTs	5
Known Issues in CTPOS Release 6.0	6
Errata in Documentation	6
Hot-Swap Feature for CTP2000 Devices	7
Resolved Issues in CTPOS Release 6.0	7
Diagnostics: Writing Logs to FLASH Before Watchdog restart	7
Reference Log Entries	8
PBS or Bridging Operation	8
CESoPSN Bundles	8
Node Summary	8
T1/E1 Interfaces	8
Virtual IP address	8
Login Banner	8
Loopback on CTP2000 and CTP150 T1/E1 Modules	8
PBS Interfaces	8
CTP and SAToP Bundles	8
CTP Documentation and Release Notes	9

Requesting Technical Support	9
Self-Help Online Tools and Resources	9
Opening a Case with JTAC	10
Revision History	11

Upgrade Notes

Because of the new features and hardware supported in CTPOS 6.0R1, a direct code upgrade by means of an upgrade archive from earlier versions of CTPOS is not supported. You must perform the upgrade CTPOS 6.0R1 by using an upgrade kit. There are two upgrade kits, the use of which depends on whether you are using a PP310 or PP332 processor in your CTP2000 series device. An upgrade guide explains how to perform and register your upgrade.

The PP310 upgrade kit contains:

- 4-GB CTPOS 6.0R1 upgrade CompactFlash card
- USB to CompactFlash adapter
- 1-GB non-ECC RAM module
- Rear transition module (RTM)
- Jumper (for BIOS reset)

The PP332 upgrade kit contains:

- 4-GB CTPOS 6.0R1 upgrade CompactFlash card
- USB to CompactFlash adapter
- 1-GB ECC RAM module

New Features

The following features have been added to CTPOS Release 6.0. Following the description is the title of the documentation to consult for further information.

CTP150 Hardware Platform

The Juniper Networks CTP150 Circuit to Packet platform is a 1-U high, full-rack wide chassis designed for tabletop or shelf installation. It can also be installed in a rack with the supplied rack-mounting kit. The CTP150 platform has two removable modules for serial interfaces, T1/E1 interfaces, or both, and a removable Type II CompactFlash card, but no hard drive. It is available in a removable AC-powered version only. [*CTP150 Circuit to Packet Platform Hardware Guide*]

Interoperability with M Series E1/T1 Circuit Emulation PICs Using SAToP Bundles

You can use SAToP bundles to allow CTP devices to interoperate with Juniper Networks T1/E1 Circuit Emulation PICs on M Series Multiservice Edge Routers.

This interoperability allows you to deploy CTP150 and CTP2000 platforms to the customer edge by connecting them to existing M Series routers. By using existing routers and circuit emulation PICs with CTP equipment, you can provide services to smaller, remote locations without having to deploy additional M Series routers.

This feature uses a static Layer 2 circuit pseudowire that supports the use of GRE tunnels for carrying MPLS pseudowire traffic. To use this feature, you create a Layer 2 circuit and a GRE tunnel between the CTP device and the CE PIC on the router. Using SAToP encapsulation, you can provide a T1 TDM transport through the GRE tunnel.

The M Series router must have tunneling services available. These services can be built-in, as with the M7i, M120, and M360, or provided if you use an advanced services (AS) PIC that supports tunneling. [*SAToP Bundle* pathway page]

Hot-Swap Interface Module Replacement on CTP2000 Devices

You can now replace the following modules on the CTP2000 device without powering down the device (hot-swap);

- CTP2000 8-port serial interface module (CTP2000-IM-8P)
- CTP2000 8-port serial interface module, including a configurable T1/E1 interface (CTP2000-IM-8P-T1)
- CTP2000 8-port serial interface module, including a configurable 4WTO interface (CTP2000-IM-8P-V)
- CTP2000 Series T1/E1 interface module (CTP2000-IM-8P-T1E1)

Before performing a hot-swap, be aware of the following restrictions:

- Hot-swapping works most efficiently when your interface module is the same type as the interface module being replaced. If your replacement interface module is a different type, you must clean up the database information for the affected slot by deleting all bundles attached to the interface module.
- Hot-swapping is not supported on slot 0, because the clock distributor uses slot 0.
- For best results, close all open menu sessions before performing a hot-swap.



NOTE: There may be a brief traffic interruption when you replace an interface module using hot-swap.

To perform hot-swapping:

1. From the Main Menu, select **4) Node Diagnostics**.
2. If you are inserting a module into an empty slot, continue with step 7.
3. Select **8) Card Swap menu**.
4. Select **1) remove**. You are prompted to enter a slot number.
5. Enter **1**. The following message is displayed: **It is now safe to remove the card from the system!**
6. Remove the interface module from the slot.
7. Plug the new or replacement interface module into the slot.
8. Press Enter.

9. Select **8) Card Swap menu**.
10. Select **2) add**. You are prompted to enter a slot number.
11. Enter a slot number from 1 to 6. The following message is displayed: **Please make sure the card is already physically inserted.**
12. Press Enter. The following message is displayed: **Card is inserted and the database is populated to the card!**
13. Quit the current menu session before resuming work by opening a new menu session.

Route Management Redundancy is Now Link State Aware

Route management redundancy for next-hop gateways (routers) is now link state aware. Previously, the route management feature used ICMP echoes to test whether the next-hop gateway was reachable. The software now also uses link-state detection to test for IP connectivity, which means that in the case of a local link failure, the failure is detected faster than with ICMP echo. [*Redundancy in the CTP Network pathway page*]

CESoPSN Bundles Now Support BERTs

You can now use the CTP Menu to run bit error rate tests (BERTs) for CESoPSN bundles.

1. From the Main Menu, select **1) Bundle Operations**.
2. Select **3) CESoPSN**.
3. Select a bundle from the list.
4. If the bundle is not active, select **4) Activate**.
5. Select **8) Runtime Diags**.
6. Configure the options as described in Table 1 on page 5.

Table 1: Setting up Diagnostic Testing for CESoPSN Bundles in the CTP Menu

Field	Function	Your Action
Serial Loop	Creates or removes a loop on the serial interface, and specifies the direction of the loop.	Select one: <ul style="list-style-type: none"> • None—Removes any active loops on the bundle. • To NET—Data arriving from the IP network destined for the serial interface is looped back to the IP network and the remote port. The data is still transmitted from the IP network to the serial interface, but the data from the serial interface to the IP network is blocked. • To I/F—Data arriving from the serial interface that is destined for the IP network is looped back to the serial interface. The data is still transmitted from the serial interface to the IP network, but the data from the IP network to the serial interface is blocked.

Table 1: Setting up Diagnostic Testing for CESoPSN Bundles in the CTP Menu (*continued*)

Field	Function	Your Action
BERT Injection	Specifies whether this bundle acts as the BERT transmitter. If the bundle is the BERT transmitter, specifies the direction in which it transmits test data.	<p>Select one:</p> <ul style="list-style-type: none"> Disabled—Disables BERT transmission on this bundle. Tx to NET—BERT pattern is injected toward the IP network. User data in this direction is replaced with the BERT pattern. User data transmitted in the direction of the IP network is replaced with the BERT pattern. Tx to I/F—BERT pattern is injected toward the serial interface. User data in this direction is replaced with the BERT pattern.
BERT Reception	<p>Specifies whether this bundle acts as the BERT receiver. If the bundle is the BERT receiver, specifies the direction from which it receives test data.</p> <p>The BERT receiver does not disrupt the existing data flow in either direction.</p>	<p>Select one:</p> <ul style="list-style-type: none"> Disabled—Disables BERT reception on this bundle. Rx from NET—BERT pattern is received from the network. Rx from I/F—BERT pattern is received from the interface.
BERT Pattern	<p>Specifies the type of BERT pattern. BERT patterns are compatible with the Firebird 6000, with the exception of 2³-1.</p> <p>You must configure the same pattern on each end of the bundle.</p>	<p>Select one:</p> <ul style="list-style-type: none"> MARK ALT 511 2047 2¹⁵-1 2²⁰-1 2²³-1 2²⁹-1 2³¹-1 2⁴-1
BERT Error Inject	Specifies whether the BERT transmitter injects an error in the pattern to verify that an end-to-end BERT has been established.	Select 5) BERT Error Inject .

Known Issues in CTPOS Release 6.0

Errata in Documentation

- Chapter 17, *Replacing Interface Modules Using Hot-Swap* describes how to replace modules on the CTPI50 device without powering down the device. This feature is not supported on CTPI50 devices in this release of the software. [Juniper Networks CTPI50 Circuit to Packet Platform Hardware Guide]
- Chapter 2, *CTPI50 Interface Modules*, contains the topic *CTPI50 Multiservice Interface Module*. The multiservice interface module is not supported in this release of the software. [Juniper Networks CTPI50 Circuit to Packet Platform Hardware Guide]
[Juniper Networks CTPI50 Circuit to Packet Platform]

Hot-Swap Feature for CTP2000 Devices

- After you perform a hot-swap on a CTP2000 device, the device may reboot after 20 minutes. [525160]

Resolved Issues in CTPOS Release 6.0

Diagnostics: Writing Logs to FLASH Before Watchdog restart

If the CTP device crashed and caused the watchdog to restart the device, logs stored in RAM were lost. [PR/449598: This issue has been resolved.]

Reference Log Entries

- If you set up advanced logging for references and a reference was lost, the log did not print for that reference. [PR/476776/510297: This issue has been resolved.]

PBS or Bridging Operation

- The display of the PBS or bridging operation listed port numbers instead of the interface. [PR/509446: This issue has been resolved.]

CESoPSN Bundles

- When you selected the option, CTP is Clock Source – Adap for CESoPSN bundles, the CTP Menu allowed you to configure Adaptive Parameters, which are not supported for CESoPSN bundles. [PR/509182: This issue has been resolved.]

Node Summary

- The Node Summary display in CTP Menu was greater than 80 characters wide. [PR/508220: This issue has been resolved.]

T1/E1 Interfaces

- After a bundle had been deleted, the port configuration was not being reset to default settings. [PR/507792: This issue has been resolved.]

Virtual IP address

- If you deleted a virtual IP address from the CTP device and a bundle was configured to use the virtual IP address, the bundle configuration was not modified to remove the address and the bundle was not disabled. [PR/509734: This issue has been resolved.]

Login Banner

- When you accessed a CTP device using SSH, the login banner did not display. [PR/516790: This issue has been resolved.]

Loopback on CTP2000 and CTP150 T1/E1 Modules

- When you set up an analog loop on CTP2000 and CTP150 T1/E1 modules, the Rx termination was not included in the loopback path, and the interface received errors. [PR/511056: This issue has been resolved.]

PBS Interfaces

- Receive (Rx) counters were not being incremented for PBS interfaces. [PR/509725: This issue has been resolved.]

CTP and SAToP Bundles

- Packet size validation was not occurring when CTP and SAToP bundles were configured through the CTP Menu. [PR/507222: This issue has been resolved.]

CTP Documentation and Release Notes

For a list of related CTP documentation, see

http://www.juniper.net/techpubs/en_US/release-independent/ctp/information-products/pathway-pages/index.html.

If the information in the latest release notes differs from the information in the documentation, follow the *CTPOS Release Notes* and the *CTPView Server Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at

<http://www.juniper.net/techpubs/>.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html> .

Revision History

June 2010—Revision 1, CTPOS 6.0

Copyright © 2010, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.