Juniper Networks® CTPOS 6.1 Software Release Notes

Release 6.1R1
January 2011
Revision 1

These release notes accompany Release 6.1R4 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/ctp6.1/information-products/pathway-pages/ctp-series/index.html.

Contents

Upgrade Information

You upgrade to CTPOS 6.1x as follows:

- If you are upgrading to CTPOS 6.1x from software releases 4.x or 5.x, you use upgrade kits to upgrade your CTP device to CTPOS6.x.
- If you are upgrading to CTPOS 6.1x from software release 6.0R1, you can use software files for the upgrade.

Upgrading from CTPOS Releases 4.x or 5.x to CTPOS 6.x with an Upgrade Kit

Because of the new features and hardware supported in CTPOS 6.x, a direct code upgrade by means of an upgrade archive from earlier versions of CTPOS is not supported. You must perform the upgrade to CTPOS 6.x 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:

CTP2000 Platform Upgrade to CTPOS 6.x

The CompactFlash card that is shipped with the upgrade kits may contain either CTPOS 6.0R1 or CTPOS 6.1x. If the CompactFlash card contains CTPOS 6.0R1, and you wish to upgrade directly to CTPOS 6.1x, you need to reburn the CompactFlash card with the CTPOS 6.1x code before you perform the upgrade.

Upgrading From CTPOS Release 6.0x to CTPOS 6.1x

To upgrade from CTPOS 6.0R1 or later, use the following files:

- CTPOS complete file (Includes all required files for upgrade): ctp_complete_6.1R4_110106.tgz
- CTP2000 Winmon Archive File: acorn_429_100331_winmon_210.tgz
- CTP2000 FPGA Archive File: acorn_429_101220_fpga_2000_ser_v74_t1e1_vEA_24.tgz
- CTP150 FPGA Archive File: acorn_429_101221_fpga_150_ser_v1e_t1e1_v1a.tgz
- CTP2000 Bios Archive File: acorn_429_101015_bios_V221.tgz
- Voice card Archive File: acorn_429_101108_em9c_fxo61_fxs50_voice.tgz
- Dcard Archive File: acorn_429_100416_dcardpld_t1e1_3_4wto_4.tgz

New Features

The following features have been added to CTPOS Release 6.1. Following the description is the title of the documentation to consult for further information.

Upgrading Boot FPGA During Interactive Mode Software Upgrade

When you run the script to upgrade your CTP device to release 6.1, you have the option to run the installation interactively:

```
Do you want to install the newest archive interactively (w/ questions)? y[n]: y
```

If you select yes, you are given to option to upgrade the boot FPGAs.

```
        Do you want to program all FPGAs without asking for each one? y[n]:
        Do you want to program boot FPGAs also? y[n]:
        Do you want to program FPGAs regardless of the existing version? y[n]:
```

Fractional T1/E1 Support on CTP150 Devices

CTP150 devices now support fractional T1 and E1 for CTP bundles. [*CTP Bundle* pathway page]

CESoPSN Bundles are Supported on T1/E1 Interfaces on CTP150 Devices

You can now configure CESoPSN bundles on T1/E1 interfaces on CTP150 devices. CTP devices support up to 16 CESoPSN bundles on an interface and up to 32 bundles on the device.

CESoPSN bundles on CTP150 devices support all of the parameters that are available on CESoPSN bundles on CTP2000 devices. In addition, CESoPSN bundles on CTP devices support the following parameters:

- Minimum buffer size
- Missing packet fill pattern
- Consecutive packets loss to starvation
- In sequence packets after starvation.

Default buffer settings for CESoPSN bundles on CTP150 devices are calculated as follows:

- If the packet size is less than 3 ms of payload, set the buffers as follows:
  - Minimum buffer=8 ms
  - Maximum buffer=16 ms
  - Packet buffer set=12 ms
- If the packet size is greater than 3 ms of payload, set the buffers as follows:
  - Minimum buffer=1 (packet time)
  - Maximum buffer=2 (packet time)
  - Packet buffer set=3 (packet time)

For example, if the packet size is 80 bytes with one channel in the bundle and signaling is off, one packet time is calculated as:

```
80/8=10 ms
```

If you set clocking for the CESoPSN bundle to **CTP is Clock Source (Adaptive End)**, the first bundle activated on the interface is assigned as the adaptive master bundle upon which the transmit clock is adjusted. This bundle is also the last bundle to be deactivated on the interface.

If the T1/E1 interface is in the loss of signal (LOS), loss of frame (LOF), or alarm indication signal (AIS) state, the bundle sets the L bit in the control word in CESoPSN packets sent to the network. This condition causes the remote end of the bundle to discard packets instead of sending them out of the interface, which in turn causes the remote bundle to stay in the In Sync state while reporting the number of transmitted packets as 0.

[CESoPSN Bundle pathway page]

Flexible Voice Compression Bundles

Previously, if you configured a Vcomp bundle on a T1/E1 interface module, all ports on the module had to be used for Vcomp bundles. You could not configure any other bundle type on the module. With the flexible Vcomp bundle feature, when you configure a Vcomp bundle on a T1/E1 module, you can specify whether the module is dedicated to only Vcomp bundles or whether other bundle types can be configured on the module.

If you are creating a new Vcomp bundle on a T1/E1 interface module and there are no other bundles configured on the interface, you are prompted to specify whether the T1/E1 interface is dedicated to Vcomp bundles.

```
Do you want to configure this card for all VCOMP?  y[n]:
```

- If you specify yes, all ports on the interface can be used for Vcomp bundles, and you cannot configure any other bundle types on the interface.
- If you specify no, you can configure other types of bundles on the interface. However, you cannot use port 2 for Vcomp bundles.

[*Vcomp Bundle* pathway page]

Y-Cable Redundancy at Both the Local and Remote Sites

Previously, the CTP Series provided Y-cable redundancy for bundle failover at the remote site. You can now use Y-cable redundancy Bundle failover for CTP bundles at both the local and the remote sites.

Additionally, 6.1 allows for diagnostics to be run on a non-active bundle attached to a Y cable without introducing data errors on the active bundle. The only caveat is that neither serial interface can have a daughter card installed

You can use Y cables only for serial CTP interfaces. There are two separate Y cables—one for CTP150 serial interfaces, the other for CTP2000 serial interfaces.

[CTP Redundancy pathway page]

Clocking changes to Y-Cable Redundancy

Support for the following clock configurations are added to Y-cable redundancy:

- Configured rate with external TX clock (TT) without the requirement to enable high TT checking.
- All clocked with external TX clock (TT).
- Adaptive clocking with external TX clock (TT).

Full Support for SSH RADIUS Access

Users can now access CTP devices using SSH with RADIUS or RSA SecurID authentication without the requirement that a local account for the user exist on the CTP device.

For this feature to work, users must have the proper CTP attributes assigned to their RADIUS accounts. Instructions for configuring RADIUS and RSA SecurID servers for use with CTP devices and CTPView servers are available in the CTPView Security Implementation Guide available here:

`http://www.juniper.net/techpubs/en_US/ctp6.1/information-products/pathway-pages/`

Because this feature introduces new configuration options, the installation script sets the RADIUS state to Disabled on the CTP device. All other settings of the current RADIUS configuration are maintained.

To configure SSH RADIUS access on a CTP device with CTPView:

1. In the side pane, select **System** > **Configuration**.
2. Click **Node Settings**.
3. Under **Radius Settings**, configure the parameters described in Table 1 on page 6, and click **Submit Settings**.

There is no option to configure RADIUS settings from the CTP Menu.

Table 1: CTP Radius Settings Available in CTPView

Field	Function	Your Action
Status	Specifies the status of the RADIUS access.	Select one: • Disabled • Enabled
Dest Port	Specifies the destination port used to connect to RADIUS servers.	Enter a port number.
Retries	Specifies the number of additional attempts the CTP device makes to query a RADIUS server when no response is received after the specified Time Out period before it moves on to the next RADIUS server in the list. The RADIUS servers are queried in order until a response is received from a server or the maximum number of retries is reached for each server.	Select a number from 0 through 9.
Off-Line Failover	Specifies the behavior when no RADIUS server responds to the login request.	Select one: • Not Allowed—The user is denied access. • Allowed to Loc Acct—The user's login credentials are passed to the local login function.

Table 1: CTP Radius Settings Available in CTPView *(continued)*

Field	Function	Your Action
Reject Failover	Specifies the behavior when RADIUS authentication fails.	Select one: • Not Allowed—The user is denied access. • Allowed to Loc Acct—The user's login credentials are passed to the local login function.
Server IP	Specifies the IP address of the RADIUS server. You can add up to 10 servers.	Enter an IP address.
Shared Secret	Specifies the shared secret for the RADIUS server.	Enter a shared secret.
Time Out	Specifies a timeout period for attempting to connect to the RADIUS server.	Select a number from 1 through 60 seconds.

Reducing the Number of SNMP Traps Generated for Late and Missing Packets

This feature is supported on SAToP and CTP bundles.

To reduce the number of SNMP traps generated for late and missing packets with the CTP Menu:

1. From the Main Menu, select **1) Bundle Operations**.
2. Select **1) CTP** or **2) SAToP**.
3. Select a bundle from the list.
4. Select **12) Missing Pkts generate snmp trap**, and configure the parameter as described in Table 2 on page 7.
5. Select **13) Late Pkts generate snmp trap**, and configure the parameter as described in Table 2 on page 7.

Table 2: SNMP Trap Parameter Settings in the CTP Menu

Field	Function	Your Action
Missing Pkts generate snmp trap	Number of packets that are missing before the CTP device generates an SNMP trap.	Enter a number from 0 through 255. 0 disables this setting. An SNMP trap is generated for each missing packet.
Late Pkts generate snmp trap	Number of packets that are late before the CTP device generates an SNMP trap. Late packets are packets that arrived too late at the CTP device to be processed out the interface.	Enter a number from 0 through 255. 0 disables this setting. An SNMP trap is generated for each missing packet.

Minimum Packet Size

Partially filled packets can now be transported over the IP network to minimize latency on low speed circuits. This feature applies to packets created by CTP bundles. The minimum packet size for CTP150 devices is reduced to 8, and the minimum packet size for CTP2000 devices is reduced to 4.

Improved Packet Protector Efficiency

The packet protector feature now has configuration options that allow the feature to work using only 50% additional bandwidth instead of 100% additional bandwidth. Previously, you only had the option to use one-for-one duplicate packets. You can now configure the packet protector to use duplicated XOR packets, which use less bandwidth. The two new options in the CTP Menu are:

- Expect cloned XOR packets—The CTP device uses cloned XOR packets that it receives when the IP network drops the original packet to regenerate the missing packet. If the device receives both the original and cloned XOR packets, it ignores the cloned packet.
- Send & expect cloned XOR packets—The CTP device sends cloned XOR packets over the IP network. The CTP device uses cloned XOR packets that it receives to regenerate missing packets when the IP network drops the original packet.

When you use cloned XOR packets, you must set your buffer sizes so that they are large enough to accommodate three packets. You can use the following formula to determine the correct buffer size:

```
3/[circuit speed/(8 * packet size)]
OR
((circuit speed / packet size)/8)=packets per second
```

For example, a circuit with a speed of 9.6k and 32-byte packets needs a minimum buffer set point that is greater than 80 ms:

```
(9600/32)/8=37.5 packets per second
1/37.5 = 26.67 ms * 3 = 80 ms
```

SNMP traps for LOS and LOF Alarms on Bundles on T1/E1 Interfaces

For bundles configured on T1/E1 interfaces, if there are loss of service (LOS) or loss of frame (LOF) alarm changes, the alarms for all bundles configured on T1/E1 interfaces on the CTP device are aggregated into one trap per second.

SNMP trap 11 is added for this feature. It reports the LOS or LOF alarm status of all ports on T1/E1 interfaces in the following format:

```
/usr/local/bin/snmptrap -v 2c -c "ctp" 10.10.62.43 " "
1.3.6.1.4.1.18841.1.2.1.6.0.11 1.3.6.1.4.1.18841.1.2.1.5.11 s "LOS 1c 00 00 00
00 00 00 LOF 00 00 00 00 00 00 00 "
```

Each byte that follows the LOS or LOF represents the status of bundles on the T1/E1 interface. For example, 1c represents that interface 0 has ports 2, 3, and 4 in LOS alarm status.

Resolved Issues in CTPOS Release 6.1

Y-Cable Redundancy

- If you configured a bundle for Y-cable redundancy, and you set clocking to Configured rate with external TX clock, you needed to enable high TT checking. This issue has been resolved.

Hot-Swap Feature for CTP2000 Devices

- After you perform a hot-swap on a CTP2000 device, the device may reboot after 20 minutes. [525160: This issue has been resolved.]

Voice Compression

- The **cmd** command for flexible voice compression does not modify the all_vcomp flag when there are multiple configuration sessions running on the CTP device. [PR/547473: This issue has been resolved]
- Vcomp bundles on CTP devices that are running CTPOS release 6.x will not interoperate with Vcomp bundles running on CTP devices that are running CTPOS release 5.x. [PR/543064: This issue has been resolved.]
- When configuring serial port se-2/3, The CTP device behaves as if the interface is a Voice compression interface and displays the following message: “Sorry, the card must be set to all VCOMP to use port 2.” [PR/535303: This issue has been resolved.]

Packet-Bearing Serial Interfaces

- Activating or Disabling a bundle on a PBS interface causes starvations on other bundles on the PBS link [PR/547220: This issue has been resolved.]
- If you have a PBS link running between two CTP devices, and you activate a CTP bundle across the link, the PBS link becomes nonfunctional and the following log messages appear:

  ```
  Sep 29 18:16:51 nova_58 kernel: Virtual device scc0 asks to queue packet!
  Sep 29 18:16:51 nova_58 last message repeated 3 times
  Sep 29 18:16:51 nova_58 kernel: NETDEV WATCHDOG: scc0: transmit timed out
  ```

  [PR/476476: This issue is resolved]

Layer 2 Aggregation

- Layer 2 Aggregation ports do not carry traffic properly. There are issues that include transmit timeouts, dropped packets, and long/corrupt packets. [PR/546460: This issue has been resolved.]

CESoPSN Bundles

- Activating a CESoPSN bundle causes the CTP device to hang. [PR/548219: This issue has been resolved.]

IPv6 only configuration

- When a CTP device is configured for IPv6 only and you add a bundle, the remote address shows an IPv4 address. [PR/538319: This issue has been resolved.]

First Boot Process After Power Cycle

- After installing CTPOS 6.0R1 and performing a firstboot process, the CTP device performs another firstboot process after the power is cycled. [PR/531623: This issue has been resolved]

High CPU Utilization

- The issue of high CPU utilization sometimes seen on CTP devices related to the daemon that listens to the Port Fowarding sockets is resolved. [PR/ 549070]

Inband Signaling

- When InBand Signaling is configured on circuit, the CTS and DCD signals toggle high for a brief time even though the input does not change on the remote end. The signal should remain and stay low because the input on the far end is low. When the signal toggles high, it will do so for a very brief period in time. [PR/570582: This issue has been resolved]

Incorrect Display of MAC Address and Running Status

- CTP devices that have a 613 FX PCI mezzanine card (PMC) module show an incorrect MAC address and running status. [This issue has been resolved.]

CTP Device Boot Issue

- CTP devices that have a 613 PMC installed on a PP332 processor and are running CTPOS 6.x code will not boot. [PR/563751: This issue has been resolved]

RAM Disk Full After CTP Device Reboot

- When a CTP device running CTPOS 6.0 is rebooted, the RAM disk can fill up to 100%. The following error is displayed.

```
awk: cmd. line:1: (FILENAME=- FNR=1) warning: error writing standard output
 (No space left on device)
```

[PR/563476: This issue has been resolved]

RADIUS Authentication

- RADIUS authentication using a console or terminal server login is not supported [PR/ 562494: This issue has been resolved]

Ungraceful Exit From SSH Sessions

- An ungraceful exit from an SSH session when other sessions exist to the same CTP device (all querying the status of a port), causing the menu to freeze and allowing no access and no response from the other sessions. [PR/ 556865: This issue has been resolved]

Known Issues in CTPOS Release 6.1

Clocking Issue with Bundles on CTP2000 Serial Interfaces

- Bundles configured on CTP2000 serial interfaces can fail when clocking is set to external TT. Bundles that fail are also typically configured for maximum speed and packet size. A reboot of the CTP device can clear up the issue for a period of time. [PR 557567]

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

January 2011—Revision 1, CTPOS 6.1R4

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.