Juniper Networks® CTPView Server Software 4.1 Release Notes

Release 4.1R1
October 2010
Revision 1

These release notes accompany Release 4.1R1 of the CTPView Network Management System Software. They contain upgrade information and describe the enhancements to the software. CTPView Release 4.1 software is compatible with Juniper Networks CTP Series platforms running CTPOS version 6.1 or earlier.

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/index.html.

Contents

Required Upgrade Files

The full suite of security enhancements is available only when the CTPView software is installed on servers running the CentOS 5.3 Operating System. Contact Juniper Networks Technical Assistance Center (JTAC) if you need to upgrade your operating system.

The following files are provided for upgrading the CTPView software:

- web_update_4.1R1_100924.tgz [Software Updates]
- ctpview_complete_centos_4.1R1_100924.tgz [Software and CentOS OS Updates]
- ctpview_complete_fc9_4.1R1_100924.tgz [Software and CentOS OS Updates]
- ctpview_complete_fc4_4.1R1_100924.tgz [Software and CentOS OS Updates]

The upgrade files that you use depends on the current CTPView server's operating system and the current CTPView software release. Use Table 1 on page 3 to determine the correct file to use.

Table 1: Determining the Required Upgrade Files for Your System

CTPView Server OS	Installed CTPView Release	File for Upgrade	Server Reboots During Upgrade?
CentOS 5.3	Any	ctpview_complete_centos_4.1R1_100924.tgz	Yes
FC9	3.4R2 or later	web_update_4.1R1_100924.tgz	No
FC9	3.4R1 or earlier	ctpview_complete_fc9_4.1R1_100924.tgz	Yes
FC4	2.2R2 or later	web_update_4.1R1_100924.tgz	No
FC4	2.2R1 or earlier	ctpview_complete_fc4_4.1R1_100924.tgz	Yes

Upgrading the CTPView Software

This topic includes the following tasks:

1. Upgrading the CTPView Software for Systems Running Version 3.4R2-p1 or 3.4R3 or Later on page 3
2. Upgrading the CTPView Software for Systems Running Version 3.4R2 or Earlier on page 4

Upgrading the CTPView Software for Systems Running Version 3.4R2-p1 or 3.4R3 or Later

To install the software for systems running 3.4R2-p1 or 3.4R3 or later:

1. Copy the **web_update** or **ctpview_complete** file to the ***/tmp*** directory on the server.
2. Log in to the server shell.
    - On CentOS systems, log in as a System Administrator.

- On FC9 or FC4 systems, switch to the root user after login.

3. Run the installation script as root: **upgrade** or as system administrator: **upgrade**.

NOTE: When upgrading CentOS 5.3 systems, you are prompted to enter the MySQL Administrator's password. This password is needed to upgrade the database structures. If you do not enter the correct password, the upgrade process continues, but the server remains usable with limited MySQL functionality. In this case, to complete the upgrade process you need to manually initiate the database structure upgrade script from the CTPView CLI menu. The path to this function is **Menu** > **MySQL Functions** > **Upgrade Database Structures**.

Upgrading the CTPView Software for Systems Running Version 3.4R2 or Earlier

To install the software using one of the **ctpview_complete** files:

1. Copy the **ctpview_complete** file to the ***/tmp*** directory on the server.
2. Log in to the server shell, and then switch to the **root** user.
3. Unpack the archive. For example, **tar -xzvf ctpview_complete_fc9_4.0R1_100924.tgz**
4. Run the upgrade script: **upgrade**

To install the software using the **web_update_4.1R1_100924.tgz** file:

1. Copy the **web_update_4.1R1_100924.tgz** file to the ***/tmp*** directory on the server.
2. Log in to the server shell, and then switch to the **root** user.
3. Run the installation script: **upgrade**.

New Features

The following features have been added to CTPView Release 4.1. Following the description is the title of the Pathway page or manual to consult for further information.

Full Support for SSH RADIUS Access

This feature is available only on CTPView servers running the CentOS operating system. Contact the Juniper Networks Technical Assistance Center (JTAC) if you need to upgrade your operating system.

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

You select and configure the SSH access options for the server in the CTPView Configuration Menu under the **AAA Functions** sections. For instructions to configure this feature on CTPView, see the *RADIUS/RSA SecurID Configuration (SSH and HTTPS)* section of 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 CTPView. All other settings of your current RADIUS/RSA configuration are maintained.

Fractional T1/E1 Support on CTP150 Devices

CTP150 devices now support fractional T1 and E1 for CTP bundles. [*CTP 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.

To set up Y-cable redundancy at both the local and remote sites, you configure two bundles—a master bundle, and a backup bundle. Each bundle follows a different path between the two sites.

The bundle configuration in CTPview has a new parameter called **Y Cable Redundancy Master** that specifies that a bundle is the master bundle. This parameter is under Advanced Options in the Port Options section of the bundle configuration.

Additionally, with 6.1R1 you can run diagnostics on a non-active bundle attached to a Y cable without introducing data errors on the active bundle if you do not 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).

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 CTPView are:

- Expect cloned XOR packets—The CTP device uses cloned XOR packets that it receives to regenerate the missing packet when the IP network drops the original 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, 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
```

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?
```

- 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]

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 as well as the following parameters:

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

You can configure the minimum buffer size with CTPView. However, you can configure the missing packet fill pattern, consecutive packets loss to starvation, and in sequence packets after starvation only by using the CTP Menu.

[*CESoPSN Bundle* pathway page]

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. [*CTP Bundle* pathway page]

Security Implementation Guide

We have updated the CTPView Security Implementation Guide. The latest version is available for download at http://www.juniper.net/techpubs/en_US/ctp6.1/information-products/pathway-pages/

Security Updates of CentOS Operating System

We have updated the CentOS operating system to incorporate patches for security vulnerabilities that have been identified since Release 3.4R3. Updates of the Fedora operating systems are no longer being provided. Contact Juniper Technical Support if you need to upgrade your operating system.

The affected applications are shown in the table below:

Application	Release 3.4R2-p1	Release 3.4R2-p2
acipd	1.0.4-7	1.04-9.2
httpd	2.2.10	2.2.15-2
krb5-libs	1.6.1-31	1.8.2-2

Application	Release 3.4R2-p1	Release 3.4R2-p2
mysql	5.0.68	5.1.49-1
openssl	0.9.8k	0.9.8n
php	5.2.9	5.2.13-1
kernel	2.6.18-128.el5	2.6.18-194.8.1.el5 *

* Red Hat applies patches to the 2.6.18 kernel instead of using newer kernel versions. See “Kernel Patches Applied from Version 2.6.18-128 to 2.6.18-194” on page 8 for a list of vulnerabilities that are addressed with this kernel version.

Kernel Patches Applied from Version 2.6.18-128 to 2.6.18-194

The updated kernel-2.6.18-194.8.1.el5 contains patches for the following CVE common Identifiers. Details on individual CVE identifiers can be found on the National Vulnerability Database website: http://web.nvd.nist.gov/view/vuln/search.

Table 2: Kernel patches applied from version 2.6.18-128 to 2.6.18-194

CVE-2010-1641	CVE-2009-4538	CVE-2009-2695	CVE-2008-5713
CVE-2010-1437	CVE-2009-4537	CVE-2009-2692	CVE-2008-5700
CVE-2010-1436	CVE-2009-4536	CVE-2009-2407	CVE-2008-5025
CVE-2010-1187	CVE-2009-4272	CVE-2009-2406	CVE-2008-4934
CVE-2010-1173	CVE-2009-4141	CVE-2009-1897	CVE-2008-4933
CVE-2010-1088	CVE-2009-4138	CVE-2009-1633	CVE-2008-3528
CVE-2010-1087	CVE-2009-4131	CVE-2009-1633	CVE-2007-5966
CVE-2010-1086	CVE-2009-4036	CVE-2009-1630	CVE-2007-4567
CVE-2010-1085	CVE-2009-4021	CVE-2009-1439	CVE-2007-3719
CVE-2010-0730	CVE-2009-4020	CVE-2009-1389	CVE-2007-3719
CVE-2010-0727	CVE-2009-3939	CVE-2009-1388	CVE-2007-3719
CVE-2010-0622	CVE-2009-3726	CVE-2009-1385	CVE-2007-3719
CVE-2010-0622	CVE-2009-3621	CVE-2009-1337	CVE-2007-3719
CVE-2010-0622	CVE-2009-3620	CVE-2009-1192	CVE-2007-3719

Table 2: Kernel patches applied from version 2.6.18-128 to 2.6.18-194 *(continued)*

CVE-2010-0415	CVE-2009-3556	CVE-2009-1072
CVE-2010-0410	CVE-2009-3547	CVE-2009-0834
CVE-2010-0307	CVE-2009-3286	CVE-2009-0748
CVE-2010-0291	CVE-2009-3080	CVE-2009-0676
CVE-2010-0291	CVE-2009-3002	CVE-2009-0675
CVE-2010-0291	CVE-2009-3002	CVE-2009-0269
CVE-2010-0291	CVE-2009-2908	CVE-2009-0065
CVE-2010-0291	CVE-2009-2849	CVE-2009-0031
CVE-2010-0291	CVE-2009-2698	CVE-2009-0028
CVE-2010-0291		
CVE-2010-0291		
CVE-2010-0291		
CVE-2010-0291		
CVE-2010-0291		
CVE-2010-0291		
CVE-2010-0008		
CVE-2010-0007		
CVE-2010-0003		

Resolved Issues in CTPView Release 4.1

- The option to select a CTP150 chassis type has been added to the **Add Remote Host** section on the **Server** > **Administration** page. [PR/530409]
- You can now access the Fractional T1/E1 and Line Coding/Connector Type options on all appropriate ports when using a T1/E1 daughter card in a CTP2000 platform. [PR/530445]
- Support in CTPView for managing Port Mirroring in CTPOS Vcomp bundles is available. [PR/541258]

- The functionality of CTP150 platforms are now properly displayed on the CTPView Plot, Monitoring and BERT pages. [PR/541317]
- The option to change the signaling value for T1 ports is now functional. [PR/546501]
- The expanded listing of Port IDs displayed when you configure a Vcomp bundle on a T1/E1 port was removed. The list is not applicable to this configuration. [PR/546505]
- The issue of bridge port circuits being misconfigured when using CTPView is resolved. The labeling of Point-to-Point Link Config options for Frame Relay Encapsulation has been updated. [PR/548659]

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

September 2010—Revision 1, CTPView Release 4.1

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.