

# CTP Series Circuit to Packet Platform

Redundancy in the CTP Network

Release

6.0



Published: 2010-06-27

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
www.juniper.net

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.

*Redundancy in the CTP Network, CTP Release 6.0, CTPView Release 4.0*

Copyright © 2010, Juniper Networks, Inc.

All rights reserved. Printed in USA.

#### Revision History

June 2010—Redundancy in the CTP Network, CTP Release 6.0, CTPView Release 4.0

The information in this document is current as of the date listed in the revision history.

## END USER LICENSE AGREEMENT

**READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE.** BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).



# Table of Contents

<b>Chapter 1</b>	<b>CTP Redundancy Overview</b> .....	<b>1</b>
	Redundancy Features Overview .....	1
	Ethernet Interface Failover Overview .....	2
	Route Management Redundancy Overview .....	2
	Bundle Failover Between CTP Devices at Alternate Sites Overview .....	2
	Bundle Failover Between CTP Devices at the Same Site Overview .....	3
	Packet Redundancy Overview .....	4
<b>Chapter 2</b>	<b>Configuring CTP Redundancy</b> .....	<b>5</b>
	Enabling Ethernet Interface Failover (CTPView) .....	5
	Configuring Route Management Redundancy .....	6
	Configuring the Default Ethernet Interface (CTP Menu) .....	6
	Configuring an Ethernet Interface With Static Routes (CTP Menu) .....	7
	Enabling Route Management Redundancy (CTPView) .....	8
	Configuring Bundle Failover Between CTP Devices at Alternate Sites (CTPView) .....	8
	Configuring Bundle Failover Between CTP Devices at the Same Site .....	10
	Configuring Y-Cable Redundancy for the Bundle (CTPView) .....	11
	Configuring Y-Cable Redundancy for the Bundle (CTP Menu) .....	12
	AutoSwitch for Bundle Failover (CTPView) .....	13
	Configuring Packet Redundancy for Circuits (CTPView) .....	15
	Configuring Packet Redundancy for Circuits (CTP Menu) .....	16
<b>Chapter 3</b>	<b>Administration</b> .....	<b>19</b>
	Checking Primary and Secondary AutoSwitch Connections for Bundles (CTPView) .....	19



## CHAPTER 1

# CTP Redundancy Overview

- Redundancy Features Overview on page 1
- Ethernet Interface Failover Overview on page 2
- Route Management Redundancy Overview on page 2
- Bundle Failover Between CTP Devices at Alternate Sites Overview on page 2
- Bundle Failover Between CTP Devices at the Same Site Overview on page 3
- Packet Redundancy Overview on page 4

## Redundancy Features Overview

---

The CTP series provides the following redundancy features:

- Ethernet interface failover—If the default Ethernet interface fails, the CTP device fails over to the next unconfigured Ethernet interface.
- Route management redundancy—If the next-hop gateway (the router) becomes unreachable, the CTP device uses configured static routes to a next-hop gateway on a different network.
- Bundle failover between CTP devices at alternate sites—If a bundle circuit fails and the CTP device becomes unreachable, the CTP device fails over to a CTP device at an alternate site.
- Bundle failover between CTP devices at the same site—If a bundle circuit fails and the CTP device becomes unreachable, the CTP device fails over to a redundant CTP device that is connected to the failed device by a Y cable.
- Packet redundancy—If packets are lost because of transmission errors, the packet protector feature can enable a possible recovery scenario.

### Related Topics

- Ethernet Interface Failover Overview on page 2
- Route Management Redundancy Overview on page 2
- Bundle Failover Between CTP Devices at Alternate Sites Overview on page 2
- Bundle Failover Between CTP Devices at the Same Site Overview on page 3
- Packet Redundancy Overview on page 4

## Ethernet Interface Failover Overview

---

When the CTP device sends traffic over the IP network, it aggregates the traffic over its Ethernet interfaces. When you configure your Ethernet interfaces, you specify which Ethernet interface is the default Ethernet interface. In the AutoSwitch configuration, you can enable failover on the default Ethernet interface. If the default Ethernet interface goes down, the CTP device switches to the next unconfigured Ethernet interface.

**Related Topics**

- Enabling Ethernet Interface Failover (CTPView) on page 5

## Route Management Redundancy Overview

---

Route management redundancy provides redundancy in case the next-hop gateway (the router) becomes unreachable.

The CTP device monitors the reachability of the next-hop gateway. If the gateway becomes unreachable, the CTP software removes the configured static route from its routing table which allows traffic to be forwarded to the configured default gateway. When you configure your Ethernet interfaces, you specify a default next-hop gateway (router) in your default Ethernet interface configuration. You can then configure additional Ethernet interfaces with static routes.

**Related Topics**

- Configuring Route Management Redundancy on page 6

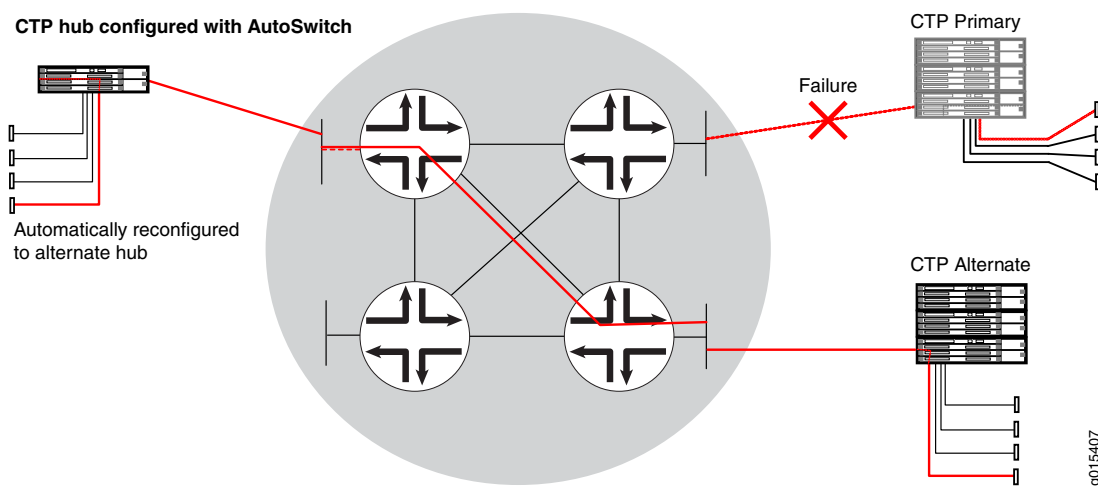
## Bundle Failover Between CTP Devices at Alternate Sites Overview

---

If a bundle circuit fails and the CTP device becomes unreachable, the CTP device can use the AutoSwitch feature to switch between primary and secondary devices.

As shown in Figure 1 on page 3, you can use this feature to automatically switch circuits from a primary site to an alternate site if a failure occurs. Automatic switching between alternate sites allows communications to be quickly restored in the event of a major site outage, as might occur with a power failure.

### Figure 1: Using Autoswitch to Back Up Bundles



For each bundle, you can have a primary and a secondary remote circuit. When you enable AutoSwitch for a bundle, it monitors the status of circuits created by the bundle. If a circuit fails to operate, the CTP software switches over to the secondary circuit on an alternate CTP device.

As shown in Figure 1 on page 3, you configure AutoSwitch at the CTP hub.

## Related Topics

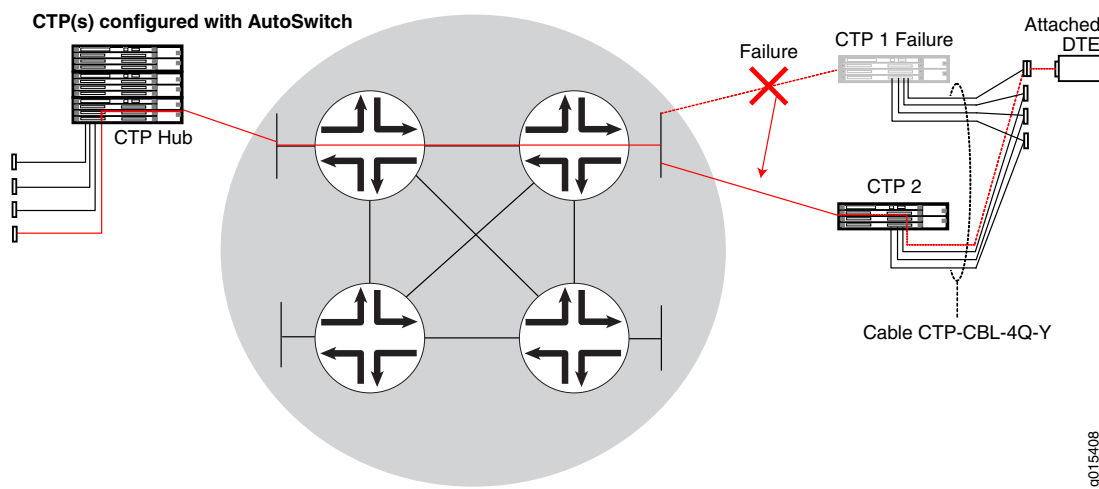
- [Configuring Bundle Failover Between CTP Devices at Alternate Sites \(CTPView\) on page 8](#)
- [Checking Primary and Secondary AutoSwitch Connections for Bundles \(CTPView\) on page 19](#)

## Bundle Failover Between CTP Devices at the Same Site Overview

Y-cable redundancy provides bundle failover using CTP devices at the same site. It provides a way to back up a CTP device with a redundant device at the same site, which increases circuit availability to a site (typically a remote site). The purpose of this redundancy scheme is to maximize network availability by providing complete hardware redundancy that protects from failures that include the network, chassis, processor, power supplies, and the interface module. It quickly restores communications when a system is not reachable or has failed, and is especially valuable at locations that do not have maintenance personnel or spare parts.

As shown in Figure 2 on page 4, during a network or equipment failure, the affected circuit is switched to a co-located alternate CTP device and port. The process of switching the circuit to the redundant system is controlled by the AutoSwitch feature running at the hub CTP system. You need to configure AutoSwitch at the CTP hub location.

Figure 2: Autoswitch with Y-Cable Redundancy



To use this feature, you use a Y cable to connect the active and standby CTP devices. With this feature enabled, the active CTP device passes data and generates keepalive messages with the standby CTP device over the Y-cable. If a failure occurs, the standby CTP device becomes active and transmits data on the circuit.

This feature requires a special Y cable (Juniper Networks part number CTP-CBL-4Q-Y). The Y cable provides control leads between the two CTP devices in addition to the standard signal, clock, and data leads connected to the attached device.

Y cable redundancy is not supported on T1 daughter cards.

## Packet Redundancy Overview

The packet protection feature increases circuit quality and reliability in IP networks that have significant packet loss.

Each circuit has IP packet redundancy to enable error-free transmission of packets. The packet protector creates and transmits one-for-one duplicate packets to the IP network. The receiving CTP device processes the redundant packets.

To use this feature, you configure packet protection on CTP, SAToP, or VComp bundles. You can specify whether each end of the connection sends and receives redundant packets.

### Related Topics

- Configuring Packet Redundancy for Circuits (CTPView) on page 15
- Configuring Packet Redundancy for Circuits (CTP Menu) on page 16

## CHAPTER 2

# Configuring CTP Redundancy

- Enabling Ethernet Interface Failover (CTPView) on page 5
- Configuring Route Management Redundancy on page 6
- Configuring Bundle Failover Between CTP Devices at Alternate Sites (CTPView) on page 8
- Configuring Bundle Failover Between CTP Devices at the Same Site on page 10
- Configuring Packet Redundancy for Circuits (CTPView) on page 15
- Configuring Packet Redundancy for Circuits (CTP Menu) on page 16

### Enabling Ethernet Interface Failover (CTPView)

This topic describes how to enable the use of Ethernet failover. You can configure this feature only in CTPView.

Before you begin:

- Log in the CTPView software at least at the Net\_Admin level.
- Connect the CTPView server to the CTP device for which you want to configure this feature.

To enable Ethernet failover using CTPView:

1. In the side pane, select **System > Configuration**.
2. Set the **AutoSwitch Daemon** parameter to Enabled.
3. Click **AutoSwitch**.
4. Under **AutoSwitch Ethernet Failover Settings**, configure the parameters described in Table 1 on page 5, and click **Submit Settings**.

Table 1: AutoSwitch Ethernet Failover Settings in CTPView

Field	Function	Your Action
Use	Specifies whether or not Ethernet failover is enabled for an Ethernet interface.  If this feature is enabled, and the active Ethernet interface goes down, the CTP device switches to an alternate Ethernet interface.	Select one: <ul style="list-style-type: none"><li>• Yes—Ethernet failover is enabled.</li><li>• No—Ethernet failover is not enabled.</li></ul>

**Related Topics** • Ethernet Interface Failover Overview on page 2

## Configuring Route Management Redundancy

Route management redundancy requires the following:

- Two Ethernet interfaces that are configured for different networks. One is the default interface that contains the default gateway configuration. The second interface provides static routes that use a different next-hop gateway.
- A virtual IP address for the CTP device. To create a list of the virtual IP addresses that will be associated with the CTP device, select **Node > Maintenance > Configure Virtual IPs**, and follow the instructions on the pane. You can create up to 56 virtual IP addresses.
- CTP bundle circuits that use route redundancy should have direct drive disabled to allow for asymmetric routing. See *Configuring IP Forwarding for CTP Bundles (CTPView)* or *Configuring IP Forwarding for CTP Bundles (CTP Menu)*

To set up route management redundancy, perform the following tasks:

1. Configuring the Default Ethernet Interface (CTP Menu) on page 6
2. Configuring an Ethernet Interface With Static Routes (CTP Menu) on page 7
3. Enabling Route Management Redundancy (CTPView) on page 8

### Configuring the Default Ethernet Interface (CTP Menu)

You are required to reboot the CTP device when you finish this configuration procedure.

To configure the default Ethernet interface using the CTP Menu:

1. From the Main menu, select **5) Node Operations**.
2. Select **3) Configure network settings**.
3. Select **2) IPv4 Configuration** or **3) IPv6 Configuration**.
4. Follow the onscreen instructions to select and specify a default Ethernet interface.
5. Configure the options as described in Table 2 on page 6.

Do not add a route to the default Ethernet interface.

**Table 2: Ethernet Interface Parameter Settings in the CTP Menu**

Field	Function	Your Action
Please input the hostname	Specifies the host name for the CTP device.	Enter a name.
Please input the ip/ipv6	Specifies the IP address of the Ethernet interface.	Enter an IP address.
Please input the netmask	For IPv4 interfaces, specifies the network mask.	Enter the network mask.
Please input the gateway	On the default Ethernet interface, specifies the IP address of the default next-hop gateway, which is the Ethernet interface on the the router.	Enter an IP address.

Table 2: Ethernet Interface Parameter Settings in the CTP Menu (*continued*)

Field	Function	Your Action
Please input the mtu in bytes	Specifies the maximum transmission unit (MTU) for the Ethernet interface.	For IPv4 networks, enter a number from 64 through 1500.  For IPv6 networks, enter a number of at least 1280.

### Configuring an Ethernet Interface With Static Routes (CTP Menu)

Configure an Ethernet interface on a network that is different from the default Ethernet interface, and add static routes to the interface configuration.

You are required to reboot the CTP device when you finish this configuration procedure.

To configure static routes for Ethernet interfaces using the CTP Menu:

1. From the Main menu, select **5) Node Operations**.
2. Select **3) Configure network settings**.
3. Select **2) IPv4 Configuration** or **3) IPv6 Configuration**.
4. Follow the onscreen instructions to select a second Ethernet interface to activate on boot, and configure the options as described in Table 3 on page 7.

Table 3: Ethernet Parameter Settings in the CTP Menu

Field	Function	Your Action
Please input the ip/ipv6	Specifies the IP address of the Ethernet interface.	Enter an IP address.
Please input the netmask	For IPv4 interfaces, specifies the network mask.	Enter the network mask.
Please input the mtu in bytes	Specifies the maximum transmission unit (MTU) for the Ethernet interface.	For IPv4 networks, enter a number from 64 through 1500.  For IPv6 networks, enter a number of at least 1280.
Add route to interface eth	Specifies whether or not to add static routes to the Ethernet configuration.	Specify <b>yes</b> .
How many routes would you like to add to eth0?	Specifies the number of static routes to add to your Ethernet interface configuration.	Enter a number between 0 and 3.
Please input the network	Specifies the IP address of the static route to the next-hop gateway.	Enter an IP address.
Please input the number of bits in the netmask	For IPv4 networks, specifies the IP mask of the Ethernet interface.	Enter an IP mask.
Please input the gateway	Specifies the IP address of the next-hop gateway (the router).	Enter an IP address.

## Enabling Route Management Redundancy (CTPView)

This topic describes how to enable the route redundancy management feature.

To enable route management redundancy using CTPView:

1. In the side pane, select **System > Configuration**.
2. Set the **AutoSwitch Daemon** parameter to Enabled.
3. Click **AutoSwitch**.
4. Under **AutoSwitch Ethernet Failover Settings**, configure the parameters described in Table 4 on page 8, and click **Submit Settings**.

Table 4: Route Management Redundancy Settings in CTPView

Field	Function	Your Action
Route Management Redundancy	Enables or disables route management redundancy	Select one: <ul style="list-style-type: none"><li>• Enabled</li><li>• Disabled</li></ul>
Check Period	<p>This parameter is under the AutoSwitch Bundle Failover Settings configuration in CTPView.</p> <p>Specifies the frequency with which the CTP software runs a reachability check. For example, if the check period is set for 30, the CTP software checks if the next-hop is reachable once every 30 seconds.</p>	Select the number of seconds.

**Related Topics**   • Route Management Redundancy Overview on page 2

## Configuring Bundle Failover Between CTP Devices at Alternate Sites (CTPView)

This topic describes how to configure AutoSwitch for bundle failover. You can configure the AutoSwitch feature only with CTPView.

Before you begin:

- Log in the CTPView software at least at the Net\_Admin level.
- Connect the CTPView server to the CTP device for which you want to configure this feature.

To configure AutoSwitch using CTPView:

1. In the side pane, select **System > Configuration**.
2. Set the **AutoSwitch Daemon** parameter to Enabled.
3. Click **Autoswitch**.

4. (Optional) You can update the network interface device (NID) information for all CTP devices that are reachable in the network. To do so, click **Update NID info** in the **Remote Host Settings** row.
5. Configure the parameters under **AutoSwitch Bundle Failover Settings** as described in Table 5 on page 9, and click **Submit Settings**.

Table 5: AutoSwitch Parameter Settings in CTPView

Field	Function	Your Action
Status	Specifies whether the AutoSwitch feature is enabled or disabled on the bundle.	Select one: <ul style="list-style-type: none"> <li>• Disabled—AutoSwitch is disabled for this bundle.</li> <li>• Enabled—AutoSwitch is enabled for this bundle.</li> </ul>
Switch Count	Specifies how many consecutive checks are required without a circuit being established before the circuit is switched over to an alternate circuit.  The combination of the switch count value and the check period value determine the rate of the switchover.	Select the number of checks.  We recommend that you configure the Switch Count and Check Period to values that prevent the circuit from switching in the event of a short transient outage.
Check Period	Specifies the time between the checking of ports to determine the circuit status.  The combination of the switch count value and the check period value determine the rate of the switchover.	Select the number of seconds.  We recommend that you configure the Switch Count and Check Period to values that prevent the circuit from switching in the event of a short transient outage.
AutoSwitch Primary	Specifies the CTP device, circuit ID, and interface that is used as the primary device to failover to.	To specify the primary device: <ol style="list-style-type: none"> <li>1. Click the box under AutoSwitch Primary, and select a group. A list of CTP devices within the group appears.</li> <li>2. Select a CTP device. A list of the circuit IDs configured on the CTP device appears.</li> <li>3. Select a circuit ID. A list of interfaces configured with the circuit ID appears.</li> <li>4. Select an interface.</li> </ol>

Table 5: AutoSwitch Parameter Settings in CTPView (*continued*)

Field	Function	Your Action
AutoSwitch Secondary	Specifies the CTP device, circuit ID, and interface that is used as the secondary device to failover to.	<p>To specify the secondary device:</p> <ol style="list-style-type: none"> <li>Click the box under AutoSwitch Primary, and select a group. A list of CTP devices within the group appears.</li> <li>Select a CTP device. A list of the circuit IDs configured on the CTP device appears.</li> <li>Select a circuit ID. A list of interfaces configured with the circuit ID appears.</li> <li>Select an interface.</li> </ol>
Secondary Revert	Specifies whether or not the CTP device periodically checks the connectivity to the AutoSwitch primary device after a switchover to the secondary device.	<p>Select one:</p> <ul style="list-style-type: none"> <li>Disabled—The CTP device does not check the connectivity to the primary device.</li> <li>Enabled—The CTP device checks the connectivity to the primary CTP device after a switchover. If the primary device becomes available, the CTP device reconnects to the primary CTP device.</li> </ul>

- Related Topics**
- Bundle Failover Between CTP Devices at Alternate Sites Overview on page 2
  - Checking Primary and Secondary AutoSwitch Connections for Bundles (CTPView) on page 19

## Configuring Bundle Failover Between CTP Devices at the Same Site

To configure bundle failover between CTP devices at the same site that are connected by a Y cable, perform the tasks below. You can configure Y-cable redundancy for the bundle using either CTPView or CTP Menu. You can configure AutoSwitch using only CTPView.

1. Configuring Y-Cable Redundancy for the Bundle (CTPView) on page 11
2. Configuring Y-Cable Redundancy for the Bundle (CTP Menu) on page 12
3. AutoSwitch for Bundle Failover (CTPView) on page 13

## Configuring Y-Cable Redundancy for the Bundle (CTPView)

Keep the following in mind when you use Y cable redundancy:

- Y cable redundancy is not supported on T1 daughter cards.
- The Y cable is short to maintain signal quality. The two CTP devices connected to the Y cable must be in close proximity to each other.
- You can use different redundant port numbers if the devices are using the same port on the 100-pin connector. For example, a Y cable 100-pin connector could be attached to ports 0-3 on the first CTP device, with the second connector attached to ports 8-11 on the second device. The redundant ports would be P0/P8, P1/P9, P2/P10 and P3/P11 on the first and second CTP devices, respectively.
- Y-cable redundancy is supported with the following clock configurations:
  - Configured rate without external TX clock (TT).
  - Configured rate with external TX clock (TT). With this option, you must enable high TT checking.
  - Adaptive clocking with internal clock.

Before you begin:

- Log in to the CTPView software at least at the Net\_Admin level.
- Connect the CTPView server to the CTP device for which you want to configure bundles.
- Disable the bundle before you modify the bundle options.

To configure advanced port options for CTP bundles using CTPView:

1. In the side pane, select **Bundle > Configuration**.
2. Run your mouse over the **Display and Select an Existing Bundle** bar.
3. In the table of bundles, select the bundle that you want to modify.
4. Under **Port Options**, place a check mark in the **Advanced Options Show** check box to display advanced parameters, and configure the parameters described in Table 6 on page 11.
5. Click **Click to Submit Bundle AND Port Changes**.
6. Configure AutoSwitch settings for bundle failover. See “Configuring Bundle Failover Between CTP Devices at Alternate Sites (CTPView)” on page 8.

**Table 6: Y-Cable Settings in CTPView**

Field	Function	Your Action
Y Cable Redundancy	Specifies whether or not a redundant Y cable is installed on the CTP device.	Select ENABLED or DISABLED.

Table 6: Y-Cable Settings in CTPView (*continued*)

Field	Function	Your Action
Only High TT Checking	<p>Specifies that the CTP device disqualifies transmit timing (TT) only when it is higher than the port speed.</p> <p>You must enable this option if you set clocking for the bundle to configured rate with external TX clock (TT).</p> <p>When enabled, this setting keeps the port from going to the TtFail state when the incoming user clock fluctuates between 0 and the configured port rate. If the TT rate goes above the configured port rate, the CTP device sends the port to the TtFail state to protect the system from an overspeed TT, which would cause problems for the port, CTP device, or network.</p>	Select ENABLED or DISABLED.

### Configuring Y-Cable Redundancy for the Bundle (CTP Menu)

Keep the following in mind when you use Y cable redundancy:

- The Y cable is short to maintain signal quality. The two CTP devices connected to the Y cable must be in close proximity to each other.
- You can use different redundant port numbers if the devices are using the same port on the 100-pin connector. For example, a Y cable 100-pin connector could be attached to ports 0-3 on the first CTP device, with the second connector attached to ports 8-11 on the second device. The redundant ports would be P0/P8, P1/P9, P2/P10 and P3/P11 on the first and second CTP devices, respectively.
- Y-cable redundancy is supported with the following clock configurations:
  - Configured rate without external TX clock (TT).
  - Configured rate with external TX clock (TT). With this option, you must enable high TT checking.
  - Adaptive clocking with internal clock.

Before you begin:

- Disable the bundle before you modify the bundle options.

To configure advanced port options for CTP bundles using the CTP Menu:

1. From the Main Menu, select **1) Bundle Operations**.
2. Select **1) CTP**.
3. Select a bundle from the list.
 

If you select an active bundle, you are prompted to disable the bundle before configuring it.
4. Select **3) Port Config**.
5. Select **4) Advanced Options**.

6. Configure the options as described in Table 7 on page 13.
7. Configure AutoSwitch settings for bundle failover. See “Configuring Bundle Failover Between CTP Devices at Alternate Sites (CTPView)” on page 8.

Table 7: Y-Cable Settings in the CTP Menu

Field	Function	Your Action
Y cable redundancy	Specifies whether or not a redundant Y cable is installed on the CTP device.	Select y or n.
Only high TT checking	<p>Specifies that the CTP device disqualifies transmit timing (TT) only when it is higher than the port speed.</p> <p>When enabled, this setting keeps the port from going to the TtFail state when the incoming user clock fluctuates between 0 and the configured port rate. If the TT rate goes above the configured port rate, the CTP device sends the port to the TtFail state to protect the system from an overspeed TT, which would cause problems for the port, CTP device, or network.</p>	Select y or n.

### AutoSwitch for Bundle Failover (CTPView)

This topic describes how to configure AutoSwitch for bundle failover. You can configure the AutoSwitch feature only with CTPView.

Before you begin:

- Log in the CTPView software at least at the Net\_Admin level.
- Connect the CTPView server to the CTP device for which you want to configure this feature.

To configure AutoSwitch using CTPView:

1. In the side pane, select **System > Configuration**.
2. Set the **AutoSwitch Daemon** parameter to Enabled.
3. Click **Autoswitch**.
4. (Optional) You can update the network interface device (NID) information for all CTP devices that are reachable in the network. To do so, click **Update NID info** in the **Remote Host Settings** row.
5. Configure the parameters under **AutoSwitch Bundle Failover Settings** as described in Table 8 on page 14, and click **Submit Settings**.

Table 8: AutoSwitch Parameter Settings in CTPView

Field	Function	Your Action
Status	Specifies whether the AutoSwitch feature is enabled or disabled on the bundle.	<p>Select one:</p> <ul style="list-style-type: none"> <li>Disabled—AutoSwitch is disabled for this bundle.</li> <li>Enabled—AutoSwitch is enabled for this bundle.</li> </ul>
Switch Count	<p>Specifies how many consecutive checks are required without a circuit being established before the circuit is switched over to an alternate circuit.</p> <p>The combination of the switch count value and the check period value determine the rate of the switchover.</p>	<p>Select the number of checks.</p> <p>We recommend that you configure the Switch Count and Check Period to values that prevent the circuit from switching in the event of a short transient outage.</p>
Check Period	<p>Specifies the time between the checking of ports to determine the circuit status.</p> <p>The combination of the switch count value and the check period value determine the rate of the switchover.</p>	<p>Select the number of seconds.</p> <p>We recommend that you configure the Switch Count and Check Period to values that prevent the circuit from switching in the event of a short transient outage.</p>
AutoSwitch Primary	Specifies the CTP device, circuit ID, and interface that is used as the primary device to failover to.	<p>To specify the primary device:</p> <ol style="list-style-type: none"> <li>Click the box under AutoSwitch Primary, and select a group. A list of CTP devices within the group appears.</li> <li>Select a CTP device. A list of the circuit IDs configured on the CTP device appears.</li> <li>Select a circuit ID. A list of interfaces configured with the circuit ID appears.</li> <li>Select an interface.</li> </ol>
AutoSwitch Secondary	Specifies the CTP device, circuit ID, and interface that is used as the secondary device to failover to.	<p>To specify the secondary device:</p> <ol style="list-style-type: none"> <li>Click the box under AutoSwitch Primary, and select a group. A list of CTP devices within the group appears.</li> <li>Select a CTP device. A list of the circuit IDs configured on the CTP device appears.</li> <li>Select a circuit ID. A list of interfaces configured with the circuit ID appears.</li> <li>Select an interface.</li> </ol>

Table 8: AutoSwitch Parameter Settings in CTPView (*continued*)

Field	Function	Your Action
Secondary Revert	Specifies whether or not the CTP device periodically checks the connectivity to the AutoSwitch primary device after a switchover to the secondary device.	Select one: <ul style="list-style-type: none"> <li>Disabled—The CTP device does not check the connectivity to the primary device.</li> <li>Enabled—The CTP device checks the connectivity to the primary CTP device after a switchover. If the primary device becomes available, the CTP device reconnects to the primary CTP device.</li> </ul>

**Related Topics** • Bundle Failover Between CTP Devices at the Same Site Overview on page 3

## Configuring Packet Redundancy for Circuits (CTPView)

The packet protector feature transmits one-for-one duplicate packets into the IP network, which enables a possible recovery scenario in the event of lost IP packets caused by transmission errors.

You can configure this feature on CTP, SAToP, and VComp bundles.

Before you begin:

- Log in to the CTPView software at least at the Net\_Admin level.
- Connect the CTPView server to the CTP device for which you want to configure this feature.

To configure redundancy for bundles using CTPView:

1. In the side pane, select **Bundle > Configuration**.
2. Run your mouse over the **Display and Select an Existing Bundle** bar.
3. In the table of bundles, select the bundle that you want to modify.
4. Under **Bundle Options**, place a check mark in the Advanced Options show check box to display advanced parameters, and configure the parameters described in Table 9 on page 16.
5. Click **Click to Submit Bundle AND Port Changes**.

Table 9: Packet Redundancy Parameter Settings in CTPView

Field	Function	Your Action
Packet Protector	<p>Specifies whether the CTP device sends and/or receives cloned (duplicated packets).</p> <p>This option is useful in networks where you expect significant IP packet loss.</p> <p>You need to configure the packet protector so that the setting at one end of the bundle corresponds with the setting at the other end of the bundle.</p> <p>For example, if you configure the local bundle to send cloned packets to the network, configure the remote bundle to expect cloned packets from the network.</p>	<p>Select:</p> <ul style="list-style-type: none"> <li>Disabled—The CTP device does not send cloned packets over the IP network, and it ignores cloned packets that it receives.</li> <li>Send cloned pkts to NET—The CTP device sends duplicated packets over the IP network.</li> <li>Expect cloned pkts from NET—The CTP device uses cloned packets that it receives when the IP network drops the original packet. If the device receives both the original and cloned packets, it ignores the cloned packet.</li> <li>Send &amp; expect cloned pkts—The CTP device sends duplicated packets over the IP network. The CTP device uses cloned packets that it receives when the IP network drops the original packet.</li> </ul>

**Related Topics** • Packet Redundancy Overview on page 4

## Configuring Packet Redundancy for Circuits (CTP Menu)

The packet protector feature transmits one-for-one duplicate packets into the IP network, which enables a possible recovery scenario in the event of lost IP packets caused by transmission errors.

You can configure this feature on CTP, SAToP, and VComp bundles.

Before you begin:

- Disable the bundle before you modify the bundle options.

To configure redundancy for CTP bundles using the CTP Menu:

1. From the Main Menu, select **1) Bundle Operations**.
2. Select the type of bundle that you want to configure.
3. Select a bundle from the list.  
If you select an active bundle, you are prompted to disable the bundle before configuring it.
4. Select **2) Config**.
5. Select **10) Advanced Options**.
6. Configure option **9) Packet Protector(tm)** as described in Table 10 on page 17.

Table 10: Packet Redundancy Parameter Settings in the CTP Menu

Field	Function	Your Action
Packet Protector(tm)	<p>Specifies whether the CTP device sends and/or receives cloned (duplicated) packets.</p> <p>This option is useful in networks where you expect significant IP packet loss.</p> <p>You need to configure the packet protector so that the setting at one end of the bundle corresponds with the setting at the other end of the bundle.</p> <p>For example, if you configure the local bundle to send cloned packets to the network, configure the remote bundle to expect cloned packets from the network.</p>	<p>Select:</p> <ul style="list-style-type: none"> <li>• Disable packet protector—The CTP device does not send cloned packets over the IP network, and it ignores cloned packets that it receives.</li> <li>• Send cloned packets to NET—The CTP device sends duplicated packets over the IP network.</li> <li>• Expect cloned packets from NET—The CTP device uses cloned packets that it receives when the IP network drops the original packet. If the device receives both the original and cloned packets, it ignores the cloned packet.</li> <li>• Send and expect cloned packets—The CTP device sends duplicated packets over the IP network. The CTP device uses cloned packets that it receives when the IP network drops the original packet.</li> </ul>

**Related Topics** • [Packet Redundancy Overview on page 4](#)



## CHAPTER 3

# Administration

- Checking Primary and Secondary AutoSwitch Connections for Bundles (CTPView) on page 19

### Checking Primary and Secondary AutoSwitch Connections for Bundles (CTPView)

---

You can test the connection between a CTP device running AutoSwitch and its primary and secondary circuits.

Before you begin:

- Log in the CTPView software at least at the Net\_Admin level.
- Connect the CTPView server to the CTP device on which you want to use this feature.

To test connections to primary and secondary circuits using CTPView:

1. In the side pane, select **System > Configuration**.
2. Click **AutoSwitch**.
3. Under **Connection Check**, you have the option of checking all connections or checking specific connections.
  - To check all connections, under **Connection Check**, click **ALL**.
  - To check connections for a specific primary or secondary circuit, click **Test** under the **Primary Host** and **Secondary Host** columns.

During the test, the buttons turn blue and display **Testing**. The results of the test are displayed inside the buttons, and the background color around the buttons either turns green for success or red for failure.

- Related Topics**
- Bundle Failover Between CTP Devices at Alternate Sites Overview on page 2
  - Configuring Bundle Failover Between CTP Devices at Alternate Sites (CTPView) on page 8

