CBA750B 3G/4G Wireless WAN Bridge Application Guide

Modified: 2018-07-09

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

CBA750B 3G/4G Wireless WAN Bridge Application Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://www.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and 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 https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page x defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/documentation/feedback/.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

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 Partner Support Service 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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

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

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 https://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 https://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Understanding the CBA750B 3G/4G Wireless WAN Bridge

CBA750B 3G/4G Wireless WAN Bridge Overview

The CBA750B mobile broadband series adapters enable easy-to-install wireless WAN connectivity in fixed business locations. For distributed enterprises like branch offices, retail stores, restaurants, and small businesses, the CBA750B provides 3G/4G wireless network connectivity to keep your business up and running.

Because third-generation (3G) wireless networks are so widely available, they have become a common deployment option for both primary and backup connectivity. The introduction of Juniper Networks CBA750B 3G/4G wireless WAN bridge offers a simple way to provide wireless connectivity as either a backup or a primary connection for branch SRX Series Services Gateways products.

This guide provides an overview that shows how to configure and deploy the CBA750B as a primary or backup 3G WAN connectivity option for Juniper Networks SRX Series Services Gateways.

Related Documentation

- Understanding the CBA750B Deployment Model on page 3
- Understanding the CBA750B 3G/4G Wireless WAN Bridge Requirements on page 6

Understanding the CBA750B Deployment Model

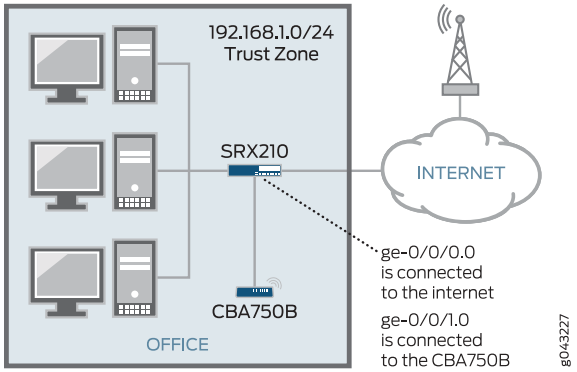
This section covers the following topics:

Deployment Model Overview

The CBA750B 3G/4G wireless WAN bridge ships with a default configuration that accommodates most deployment scenarios. The deployment model assumes that the CBA750B is connected to a DHCP-enabled interface.

Figure 1 on page 4 shows the model for the CBA750B deployment scenarios.

Figure 1: Deployment Model for the CBA750B



The CBA750B maintains the wireless modem (or modems, if more than one modem is used) in a disconnected state, triggering a new connection as soon as the SRX Series Services Gateway requests a new lease. The modem(s) are disconnected as soon as the lease expires and are reconnected only when the services gateway requires another new lease.

When you are using the 3G link as the primary connection, long lease times can be used, as generally there will not be a need to constantly connect and disconnect the line. On the other hand, if the CBA750B is used to provide a backup connection, short lease times (approximately 1 minute) are commonly used when the primary link is active. In the worst-case scenario, when the lease expires, the backup link can be disabled, triggering a disconnection.

The CBA750B assigns the address received from the wireless service provider to the services gateway (normally a public address). Only a single device can be connected to the CBA750B at a time. Otherwise, multiple devices will reject the address passed to the CBA750B. The CBA750B operates in passthrough mode to relay all traffic from the wireless network to the DHCP client.

NOTE: **The Juniper Networks CBA750B 3G/4G wireless WAN bridge supports passthrough mode only and does not support router mode. Ensure that the Router/Passthrough switch on the CBA750B right side panel is always set to the 1 position.**

CBA750B Management Interface

The CBA750B provides a Web-based management interface that is accessible even when 3G modems are not used. Because passthrough mode is used instead of a routed connection bridge, which does not perform Network Address Translation (NAT), the management interface cannot be accessed through the normal data channel.

The management interface is still accessible through the Ethernet port. Table 3 on page 5 lists the parameters that VLAN tagging uses to separate management traffic from data traffic.

Table 3: Management Network Parameters

Card Model	Wireless Technology
Management subnet	192.168.0.0/24
Management address	192.168.0.1
VLAN ID	3900

Power over Ethernet

When available, Power over Ethernet (PoE) can be used to power the CBA750B. If the CBA750B is connected through a switch or a gateway that does not support PoE, an external power supply can be used (provided with the basic install kit).

When PoE is used, the device will require about 3.5 W of power per modem connected, so plan your power budget accordingly.

Dial Modes

The CBA750B can be configured in two modes:

- Always on—the CBA750B connects to the 3G network after booting. The connection is always maintained, as long as there are no network or connectivity problems.
- Dial-on-demand—the CBA750B initiates a connection when it receives traffic from the interface connecting the CBA750B and services gateway. DHCP request messages trigger a connection, and the connection is dropped after a configurable inactivity timeout has elapsed.

Regardless of the mode, the CBA750B can accept multiple cards simultaneously. In the event of a failure or other inability to connect, the remaining card(s) are used. You can configure the connection priority through the CBA750B's management interface.

When shipped, the CBA750B is configured for dial-on-demand mode and set at 20 minutes idle timeout by default. Most carriers prefer the modem to disconnect if there is no interesting traffic. After the modem times out, DHCP requests from the SRX Series Services Gateway will result in a 192.168.30.x/24 response from the CBA750B. If interesting traffic is observed by the CBA750B, the modem attempts to connect again. Modem connection takes about 15 to 20 seconds generally. After that, the next DHCP request

from the SRX Series Services Gateway will fetch the actual 3G IP address, and Internet connection is reestablished.

Related Documentation

- CBA750B 3G/4G Wireless WAN Bridge Overview on page 3
- Understanding the CBA750B 3G/4G Wireless WAN Bridge Requirements on page 6

Understanding the CBA750B 3G/4G Wireless WAN Bridge Requirements

Table 4 on page 6 lists the requirements for deploying the CBA750B 3G/4G wireless WAN bridge.

Table 4: CBA750B 3G/4G Wireless WAN Bridge Deployment Requirements

Requirement	Description
Hardware	Juniper Networks branch SRX Series Services Gateways.
Software	• Juniper Networks Junos OS Release 10.1R1 or later • Juniper Networks Junos OS Release Junos 12.1X47-D20 or later • CBA750B firmware 5.0 or later
Card Compatibility	Many USB and ExpressCard modems have been certified to work with the CBA750B.
Card Activation	Before cards can be used, they need to be programmed with the subscriber information required to access the service provider's network. This is normally referred to as the card activation process. When a service is purchased, the carrier will request the card's ESN number, normally found printed on the wireless card. This number is then used for card identification by the different activation protocols. Cards directly purchased from the wireless carrier can ship preactivated or sometimes with a companion software used to perform the initial activation. In either case, cards that are already activated do not need to be reactivated.

Related Documentation

- CBA750B 3G/4G Wireless WAN Bridge Overview on page 3
- Understanding the CBA750B Deployment Model on page 3

PART 2

Configuring the CBA750B 3G/4G Wireless WAN Bridge with the SRX Services Gateway

CHAPTER 2

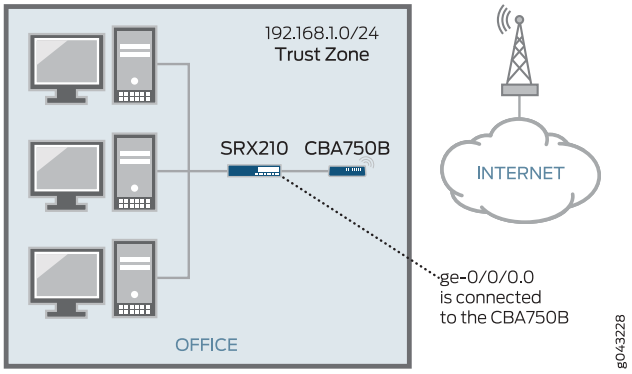
Deployment Scenarios

Using the CBA750B 3G/4G Wireless WAN Bridge for Primary Connectivity

This scenario shows the gateway configuration when the 3G network is used as the primary WAN link. This can be achieved by connecting the CBA750B 3G/4G wireless WAN bridge to any interface in the untrust zone. On the SRX210 Services Gateway, this is ge-0/0/0 when using the default configuration.

Figure 2 on page 9 shows the 3G network used as the primary WAN link.

Figure 2: 3G Network Used as the Primary WAN Link



The default configuration is as follows for completeness:

```
set system services dhcp router 192.168.1.1
set system services dhcp pool 192.168.1.0/24 address-range low 192.168.1.2
set system services dhcp pool 192.168.1.0/24 address-range high 192.168.1.254
set system services dhcp propagate-settings ge-0/0/0.0
set interfaces interface-range interfaces-trust member ge-0/0/1
set interfaces interface-range interfaces-trust member fe-0/0/2
set interfaces interface-range interfaces-trust member fe-0/0/3
```

```
set interfaces interface-range interfaces-trust member fe-0/0/4
set interfaces interface-range interfaces-trust member fe-0/0/5
set interfaces interface-range interfaces-trust member fe-0/0/6
set interfaces interface-range interfaces-trust member fe-0/0/7
set interfaces interface-range interfaces-trust unit 0 family ethernet-switching vlan members
vlan-trust
set interfaces ge-0/0/0 unit 0 set interfaces vlan unit 0 family inet address 192.168.1.1/24
set security nat source rule-set trust-to-untrust from zone trust
set security nat source rule-set trust-to-untrust to zone untrust
set security nat source rule-set trust-to-untrust rule source-nat-rule match source-address
0.0.0.0/0
set security nat source rule-set trust-to-untrust rule source-nat-rule then source-nat interface
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces vlan.0
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic
system-services dhcp
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic
system-services tftp
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
destination-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match application
any
set security policies from-zone trust to-zone untrust policy trust-to-untrust then permit
set vlans vlan-trust vlan-id 3 set vlans vlan-trust l3-interface vlan.0
```

Enabling PoE

On SRX Series Services Gateways, it is possible to use PoE to power the CBA750B. The default configuration has PoE enabled on every PoE-capable interface, requiring you only to connect the CBA750B to a PoE-capable port. Enabling PoE requires only the addition of the following configuration:

```
/* The priority is optional but it will make sure that, if too many devices are being powered,
the bridge will be given a high priority and will not be powered off */
set poe interface ge-0/0/0 priority high
```

Related Documentation

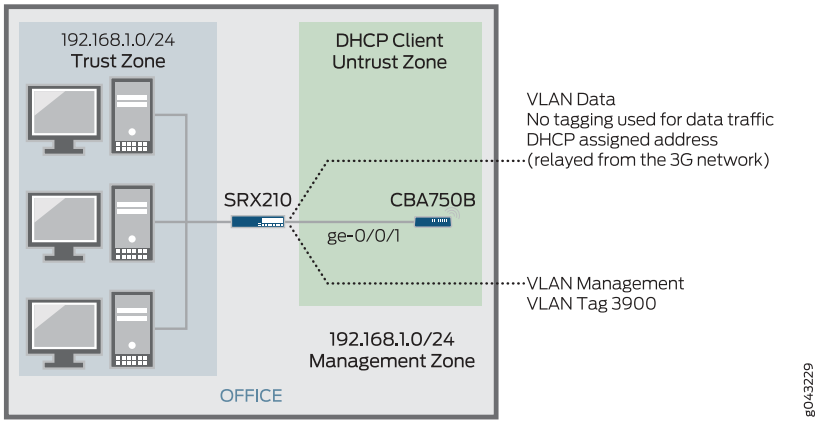
- CBA750B 3G/4G Wireless WAN Bridge Overview on page 3
- Understanding the CBA750B Deployment Model on page 3
- Using the CBA750B 3G/4G Wireless WAN Bridge for Management Access on page 11
- Using the CBA750B 3G/4G Wireless WAN Bridge for Backup on page 13
- Using RPM Probes for Detecting Network Failures on page 14

Using the CBA750B 3G/4G Wireless WAN Bridge for Management Access

A VLAN-tagged logical interface can be used to provide access to the CBA750B 3G/4G wireless WAN bridge's management console. NAT can also be used to facilitate access from any back-end device apart from the services gateway, eliminating the need for complex routing (all traffic to the CBA750B's management interface is translated as if it originated from the management subnet).

Figure 3 on page 11 shows the CBA750B management access.

Figure 3: CBA750B Management Access




```
/* The vlan.2 interface is the L3 interface of the data VLAN, connecting to the Bridge */
set system services dhcp propagate-settings vlan.2
/* Interface ge-0/0/0 has 2 VLANS configured, data and management */
set interfaces ge-0/0/0 description "Connection to CBA750B"
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members data
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members management
set interfaces ge-0/0/0 unit 0 family ethernet-switching native-vlan-id data
/* vlan.0 connects to the untrust network */
set interfaces vlan unit 0 family inet address 192.168.1.1/24
/* vlan.2 connects to the bridge (untagged) */
set interfaces vlan unit 2 family inet dhcp client-identifier ascii SRX-GW
/* vlan.3900 connects to the bridge's management subnet */
set interfaces vlan unit 3900 family inet address 192.168.0.2/24
/* VLANs */
set vlans data vlan-id 2
set vlans data l3-interface vlan.2
set vlans management vlan-id 3900
set vlans management l3-interface vlan.3900
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface vlan.0
/* NAT rule for Internet access */
set security nat source rule-set trust-to-untrust from zone trust
set security nat source rule-set trust-to-untrust to zone untrust
```

```
set security nat source rule-set trust-to-untrust rule source-nat-rule match source-address
0.0.0.0/0
set security nat source rule-set trust-to-untrust rule source-nat-rule then source-nat interface
/* NAT rule used for management access to the CBA750B*/
set security nat source rule-set trust-to-management from zone trust
set security nat source rule-set trust-to-management to zone management
set security nat source rule-set trust-to-management rule nat-to-CBA750B match
source-address 0.0.0.0/0
set security nat source rule-set trust-to-management rule nat-to-CBA750B match
destination-address 0.0.0.0/0
set security nat source rule-set trust-to-management rule nat-to-CBA750B then source-nat
interface
/* Security policies and zones */
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces vlan.0
set security zones security-zone untrust interfaces vlan.2 host-inbound-traffic
system-services dhcp
set security zones security-zone untrust interfaces vlan.2 host-inbound-traffic
system-services tftp
set security zones security-zone management interfaces vlan.3900
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
destination-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match application
any
set security policies from-zone trust to-zone untrust policy trust-to-untrust then permit
set security policies from-zone trust to-zone management policy
CBA750B-management-access match source-address any
set security policies from-zone trust to-zone management policy
CBA750B-management-access match destination-address any
set security policies from-zone trust to-zone management policy
CBA750B-management-access match application junos-http
set security policies from-zone trust to-zone management policy
CBA750B-management-access match application junos-ping
set security policies from-zone trust to-zone management policy
CBA750B-management-access then permit
```

Related Documentation

- CBA750B 3G/4G Wireless WAN Bridge Overview on page 3
- Understanding the CBA750B Deployment Model on page 3
- Using the CBA750B 3G/4G Wireless WAN Bridge for Primary Connectivity on page 9
- Using the CBA750B 3G/4G Wireless WAN Bridge for Backup on page 13
- Using RPM Probes for Detecting Network Failures on page 14

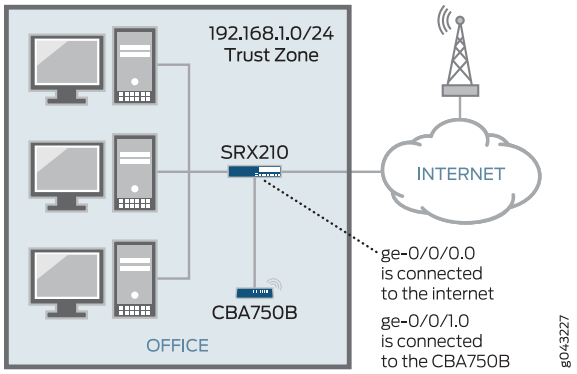
Using the CBA750B 3G/4G Wireless WAN Bridge for Backup

In this scenario, the CBA750B 3G/4G wireless WAN bridge will only be used when the primary interface is down. This is shown mostly for illustrative purposes, because only a failure in the primary interface triggers a failover.

Also, this scenario can only be used with the CBA750B operating in the *always on* mode, because once the bridge is connected, DHCP requests from the SRX Series Services gateway will keep the connection up. We do not recommend that you increase the lease times, because after a new connection the modem might not be assigned the same IP address. This scenario calls for short lease times to ensure that the gateway is notified of address changes.

Figure 4 on page 13 shows the interface backup.

Figure 4: Interface Backup



The complete default configuration is as follows:

```
/* Interface Configs */
set interfaces interface-range Trust member-range fe-0/0/2 to fe-0/0/6
set interfaces interface-range Trust unit 0 family ethernet-switching port-mode access
set interfaces interface-range Trust unit 0 family ethernet-switching vlan members Trust
/* Main Internet Link */
set interfaces ge-0/0/0 unit 0 family inet address 198.0.0.2/24
/* CBA750B backup link */
set interfaces ge-0/0/1 unit 0 family inet dhcp
set vlans default l3-interface vlan.1
set interfaces vlan unit 1 description Trust
set interfaces vlan unit 1 family inet address 192.168.1.1/24
/* Default route points to the primary link and it takes precedence over the DHCP assigned
default */
set routing-options static route 0.0.0.0/0 next-hop 198.0.0.1
/* NAT Configuration */
set security nat source rule-set Outbound-NAT from zone trust
set security nat source rule-set Outbound-NAT to zone untrust
set security nat source rule-set Outbound-NAT rule Nat-All match source-address 0.0.0.0/0
```

```
set security nat source rule-set Outbound-NAT rule Nat-All match destination-address
0.0.0.0/0
set security nat source rule-set Outbound-NAT rule Nat-All then source-nat interface
/* Security Zones */
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic
system-services ping
set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic
system-services dhcp
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces vlan.1 host-inbound-traffic system-services
dhcp
set security zones security-zone trust interfaces vlan.1 host-inbound-traffic system-services
ping
set security zones security-zone trust interfaces vlan.1 host-inbound-traffic system-services
ssh
/* Allow outboud traffic from trust to untrust */
set security policies from-zone trust to-zone untrust policy permit-outbound match
source-address any
set security policies from-zone trust to-zone untrust policy permit-outbound match
destination-address any
set security policies from-zone trust to-zone untrust policy permit-outbound match
application any
set security policies from-zone trust to-zone untrust policy permit-outbound then permit
```

Related Documentation

- CBA750B 3G/4G Wireless WAN Bridge Overview on page 3
- Understanding the CBA750B Deployment Model on page 3
- Using the CBA750B 3G/4G Wireless WAN Bridge for Primary Connectivity on page 9
- Using the CBA750B 3G/4G Wireless WAN Bridge for Management Access on page 11
- Using RPM Probes for Detecting Network Failures on page 14

Using RPM Probes for Detecting Network Failures

A primary interface's status is not always a good indicator of a network's connectivity. In some instances, when Layer 2 protocols are unable to detect end-to-end failures, or when multiple network hops separate the services gateway from remote resources, other means of triggering a failover are desired.

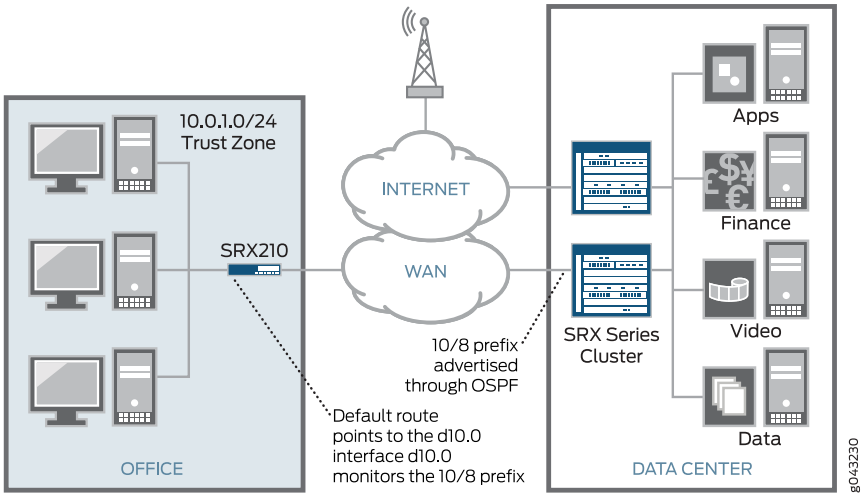
This example shows how to configure a set of watch prefixes that when they are not present in the routing table, will enable the dialer interface. Static routing with Bidirectional Forwarding Detection (BFD) or routing protocols can be used to dynamically change the status of the routes in the routing table.

The main advantage of this approach is that real-time performance monitoring (RPM) probes do not require any special routing protocol support or the use of BFD. RPM probes can be configured to use standard Internet Control Message Protocol (ICMP) messages,

HTTP get requests, or TCP/UDP pings to verify end-to-end connectivity. The RPM monitor scripts can be downloaded from the following URL: www.juniper.net/support/downloads/

Figure 5 on page 15 shows the watch prefix.

Figure 5: Watch Prefix



Even though this example builds on the scenarios already described ("Using the CBA750B 3G/4G Wireless WAN Bridge for Primary Connectivity" on page 9, "Using the CBA750B 3G/4G Wireless WAN Bridge for Management Access" on page 11, and "Using the CBA750B 3G/4G Wireless WAN Bridge for Backup" on page 13), the following configuration represents a complete working scenario:

```
/* Enable the commit script. The commit script must be stored under
/var/db/scripts/commit */
set system scripts commit allow-transients
set system scripts commit file rpm-monitor-config.xslt
/* Enable the event script. The script file must be stored under /var/db/scripts/event */
set event-options event-script file rpm-monitor.xslt
/* Local dhcp server configuration */
/* This server assigns addresses to the hosts in the Trust network */
set system services dhcp pool 192.168.1.0/24 address-range low 192.168.1.2
set system services dhcp pool 192.168.1.0/24 address-range high 192.168.1.254
set system services dhcp pool 192.168.1.0/24 router 192.168.1.1
/* This configuration creates a log file named rpm-monitor containing the login messages
from the script */
set system syslog file rpm-monitor user warning
set system syslog file rpm-monitor match cscript
/* Interface Configs */
set interfaces interface-range Trust member-range fe-0/0/2 to fe-0/0/6
set interfaces interface-range Trust unit 0 family ethernet-switching port-mode access
set interfaces interface-range Trust unit 0 family ethernet-switching vlan members Trust
set interfaces ge-0/0/0 unit 0 family inet address 198.0.0.2/24
set interfaces vlan description CBA750B-data
set interfaces vlan unit 1 description Trust
```

```
set interfaces vlan unit 1 family inet address 192.168.1.1/24
set vlans default l3-interface vlan.1
/* The backup interface should be normally disabled */
/* The monitoring scripts point to an RPM probe and, if the probe fails, the script will enable
the backup interface */
set interfaces ge-0/0/1 unit 0 apply-macro rpm-monitor-server1 test-name server1
set interfaces ge-0/0/1 unit 0 apply-macro rpm-monitor-server1 test-owner
rpm-monitor-probes
set interfaces ge-0/0/1 unit 0 disable
set interfaces ge-0/0/1 unit 0 family inet dhcp
/* RPM probe configuration */
/* Note that we are using the primary link address as the source so, when the backup link
is enabled, the probes will still fail unless the primary link comes back up. This script pings
destination 'target' address. Wait for 5' ping failures and has a '5 second' probe interval.
After 5 pings, the test waits for 15seconds before starting the pings again.*/
set services rpm probe rpm-monitor-probes test server1 probe-type icmp-ping
set services rpm probe rpm-monitor-probes test server1 target address 96.17.23.148
set services rpm probe rpm-monitor-probes test server1 probe-count 5
set services rpm probe rpm-monitor-probes test server1 probe-interval 5
set services rpm probe rpm-monitor-probes test server1 test-interval 15
set services rpm probe rpm-monitor-probes test server1 source-address 10.0.1.20
/* Default route pointing to the primary link */
set routing-options static route 0.0.0.0/0 next-hop 198.0.0.1
/* NAT configuration */
set security nat source rule-set Outbound-NAT from zone trust
set security nat source rule-set Outbound-NAT to zone untrust
set security nat source rule-set Outbound-NAT rule Nat-All match source-address 0.0.0.0/0
set security nat source rule-set Outbound-NAT rule Nat-All match destination-address
0.0.0.0/0
set security nat source rule-set Outbound-NAT rule Nat-All then source-nat interface
* Zones and policies */
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic
system-services ping
set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic
system-services dhcp
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces vlan.1 host-inbound-traffic system-services
dhcp
set security zones security-zone trust interfaces vlan.1 host-inbound-traffic system-services
ping
set security zones security-zone trust interfaces vlan.1 host-inbound-traffic system-services
ssh
set security policies from-zone trust to-zone untrust policy permit-outbound match
source-address any
set security policies from-zone trust to-zone untrust policy permit-outbound match
destination-address any
set security policies from-zone trust to-zone untrust policy permit-outbound match
application any
```

set security policies from-zone trust to-zone untrust policy permit-outbound then permit

Monitoring

The 3G signal strength and connection status can be monitored from the CBA750B's management interface, in the Device Information section under Status -> Internet Connections.

Traffic statistics can be found under Status -> Statistics.

When using the RPM monitor scripts, it is useful to look at the script logs. These logs record events such as probe failures, enabling/disabling of the backup interface, and so on. Using the configuration shown in the example, the logs can be viewed with the **show log rpm-monitor** command.

```
# run show log rpm-monitor
Jan 22 05:15:48 SRX210-Home cscript: rpm-monitor: Triggered by ping_test_up test server1
owner rpm-monitor-probes
Jan 22 05:15:48 SRX210-Home cscript: rpm-monitor: RPM probe up flagged, but there is
nothing to do with the logical interfaces Jan 22 05:16:59 SRX210-Home cscript: rpm-monitor:
Triggered by ping_test_up test server1 owner rpm-monitor-probes
Jan 22 05:16:59 SRX210-Home cscript: rpm-monitor: RPM probe up flagged, but there is
nothing to do with the routes
```

The result of the RPM probes can be viewed with the following command:

```
pato@SRX210-Home# run show services rpm history-results
Owner, Test Probe received Round trip time
rpm-monitor-probes, server1 Fri Jan 22 05:29:40 2010 192057 usec
rpm-monitor-probes, server1 Fri Jan 22 05:29:45 2010 194821 usec
rpm-monitor-probes, server1 Fri Jan 22 05:29:50 2010 197966 usec
rpm-monitor-probes, server1 Fri Jan 22 05:29:55 2010 188755 usec
rpm-monitor-probes, server1 Fri Jan 22 05:30:00 2010 189775 usec
rpm-monitor-probes, server1 Fri Jan 22 05:30:16 2010 199006 usec
rpm-monitor-probes, server1 Fri Jan 22 05:30:21 2010 190135 usec
rpm-monitor-probes, server1 Fri Jan 22 05:30:26 2010 190896 usec
rpm-monitor-probes, server1 Fri Jan 22 05:30:31 2010 192937 usec
rpm-monitor-probes, server1 Fri Jan 22 05:30:36 2010 203084 usec
```

Related Documentation

- CBA750B 3G/4G Wireless WAN Bridge Overview on page 3
- Understanding the CBA750B Deployment Model on page 3
- Understanding the CBA750B 3G/4G Wireless WAN Bridge Requirements on page 6
- Using the CBA750B 3G/4G Wireless WAN Bridge for Primary Connectivity on page 9
- Using the CBA750B 3G/4G Wireless WAN Bridge for Management Access on page 11
- Using the CBA750B 3G/4G Wireless WAN Bridge for Backup on page 13