JUNIPER NETWORKS | Engineering Simplicity

Network Configuration Example

Configure WAN Link with LTE Backup in Active/Standby Mode

Published
2023-08-28

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

Network Configuration Example Configure WAN Link with LTE Backup in Active/Standby Mode

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://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

This document describes how to build cost-efficient and self-driving network solutions for remote offices. It shows how to set up primary WAN and backup LTE connections on SRX Series Services Gateways. You use these connections to provide wired and wireless Internet and Intranet access to employees on-site, as well as wireless Internet access to guest devices.

1

CHAPTER

Configure WAN Link with LTE Backup in Active/Standby Mode

About This Network Configuration Example

This Network Configuration Example (NCE) describes how to build cost-efficient and self-driving network solutions for remote offices. It shows how to set up primary WAN and backup LTE connections on branch SRX Series Services Gateways. You use these connections to provide wired and wireless Internet and Intranet access to employees on-site, as well as wireless Internet access to guest devices. Financial and operational benefits of this use case include lower WAN operational expenditures (OpEx), lower capital expenditures (CapEx), and automated provisioning.

Use Case Overview

The proliferation of 4G LTE cellular networks, the decreased form factor and the cost of LTE-capable devices are a springboard for rapid deployment of new branch offices. LTE networks enable broadband access to the Internet and let you avoid the cost of building redundant physical infrastructure at remote office sites. You can leverage the connectivity as backup for locations that are already equipped with primary wired connections through 4G cellular networks.

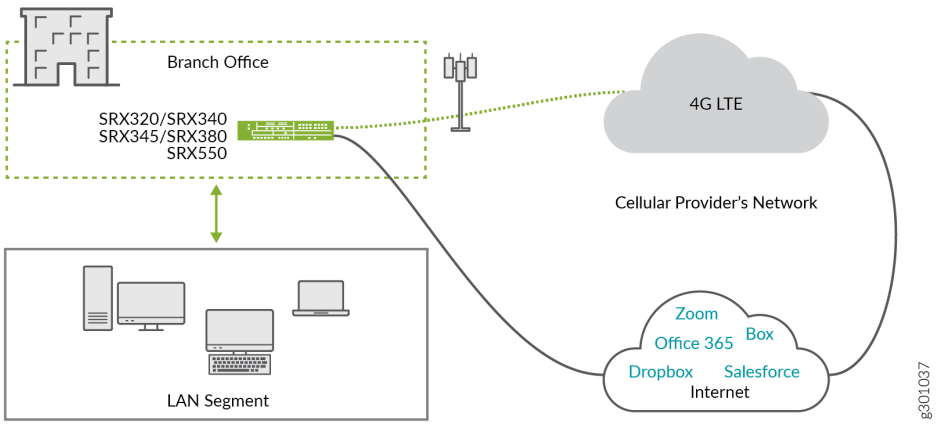
Many organizations have also made the jump to software-defined WANs (SD-WANs). They adopted the technology for business agility and responsiveness to keep up with IT innovations.

You can combine the following capabilities on the SRX300 line of devices to build cost-efficient and self-driving network solutions for remote offices:

- Firewall
- Router with redundant access to the Internet
- Advanced SD-WAN capabilities

Figure 1 on page 3 shows a typical setup of a branch office.

Figure 1: Branch Office with Redundant Internet Connectivity



A typical branch office has two independent connections to the Internet. One connection is wired and the other one is wireless, with either 2G, 3G, or 4G LTE. The connections terminate on an SRX Series device in the role of a next-generation firewall (NGFW) security appliance. This provides many wireline or wireless services to employees on-site, including:

- SD-driven access to the Internet
- Next-generation firewall:
  - Antivirus applications
  - Enhanced web filtering
  - Intrusion prevention system
  - Advanced application visibility and control

The throughput capacity of the two Internet links is often not equal, the primary link provides more throughput, compared to the standby link. The standby link usage in only when the primary link is unavailable. Because of the different capacities, you need to prioritize business critical applications over other traffic when the primary link fails. Noncritical applications can use the spare throughput capacity; therefore you can rate limit the standby link to lessen their impact on prioritized traffic.

Configuration of the MPLS link, WAN technologies, similar to Asymmetric digital subscriber line (ADSL), very-high-bit-rate digital subscriber line (VDSL), and T1/E1 are beyond the scope of this document.

Technical Overview

IN THIS SECTION

SD-WAN Overview

SD-WAN is an automated, programmatic approach to managing enterprise network connectivity and circuit costs. It extends software-defined networking (SDN) into an application that businesses can use to quickly create a smart WAN. The smart WAN comprises business-grade IP VPN, broadband Internet, and wireless services. Traffic is dynamically forwarded across the most appropriate and efficient WAN path based on network conditions, the security and QoS requirements of the application traffic, and cost of the circuit. You can set routing policies that determine how traffic is forwarded.

LTE Mini-Physical Interface Module Mini-PIM Overview

The LTE Mini-Physical Interface Module (Mini-PIM) provides wireless WAN support on the SRX320, SRX340, SRX345, SRX380 and SRX550M (High Memory) Services Gateways. The LTE Mini-PIM operates on both 3G and 4G networks. The Mini-Pim is available in two variations:

- SRX-MP-LTE-AE, which is targeted for North America and the European Union
- SRX-MP-LTE-AA, which is targeted for Asia and Australia

The main difference between the two variants is the LTE bands they operate on. You can configure LTE Mini-PIMs in three modes, **Always-on**, **Dial-on-demand**, and **Backup**. We've used **Backup** mode of operation in this NCE.

RELATED DOCUMENTATION

Configuring LTE Interfaces

Configure a WAN Link with LTE Backup in Active/Standby Mode to the Internet

IN THIS SECTION

This example shows how to configure a WAN link with LTE backup in Active/Standby setup on the SRX line of devices.

Requirements

This example uses the following hardware and software components.

- One device from the SRX300 line of devices (SRX320, SRX340, SRX345, SRX380, or SRX550)
- One LTE Mini-PIM
- One SIM card with subscription for data services

This example requires installation of an application identification license, and the download and install of the application identification package. See Licenses for SRX Series for more information. Use the `show system license` and the `show services application-identification status` commands to confirm licensing status.

NOTE: Updates to the Junos OS application signature package is authorized by a separately licensed subscription service. You must install the application identification application signature update license key on your device to download and then install the signature database updates

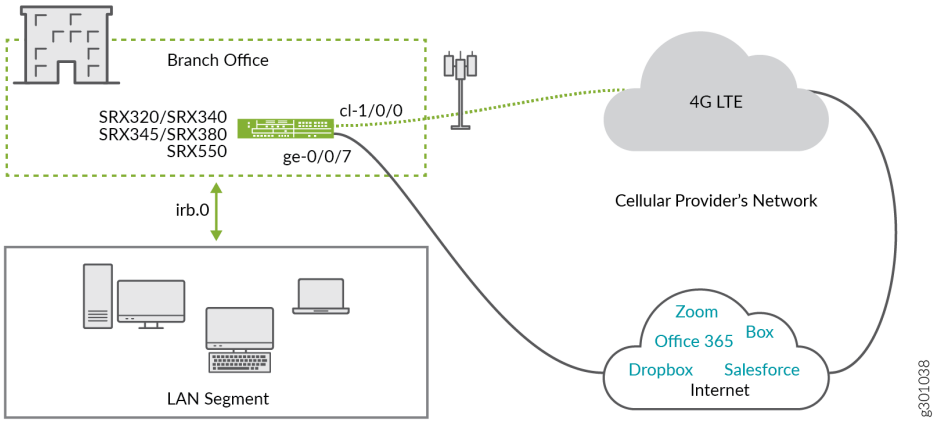
provided by Juniper Networks. When your license key expires, you can continue to use the locally stored application signature package contents but you cannot update the package.

Overview

In this example, we are setting up an SRX device to provide wired and wireless Internet and Intranet access to the employees on-site, as well as wireless Internet access to guest devices. The primary internet link is through Ethernet, while the backup connectivity is through the LTE network. The two links are configured in active/standby mode; no traffic is routed through the LTE modem (LTE-MPIM), unless the primary link is down.

Figure 2 on page 6 shows the topology of this example.

Figure 2: Branch Office with Redundant Internet Connectivity Example



Following are the topology details:

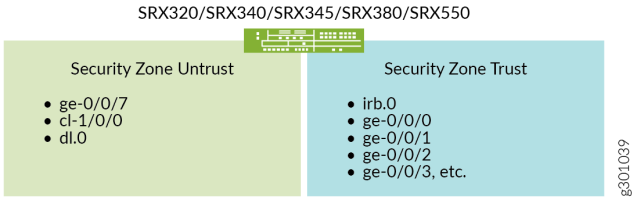
- The LTE Mini-PIM is installed in slot 1 of the SRX device.
- The SIM card is installed in slot 1 of the LTE module.
- The primary link is connected to interface ge-0/0/7.
- The primary link receives IP address, network mask, default gateway and DNS servers from the device that it is connected to.
- The interface cl-1/0/0 identifies the modem (LTE-MPIM).

The LTE network terminates the link over the cellular network on interface dl.0, and assigns the IP address, network mask, and default gateway to ge-0/0/7.

There are two security zones, untrust and trust configured on the SRX device. The separation of the interfaces into security zones enables the separation of traffic and lowers the risks that the corporate Intranet is exposed to. Security zones serve as a vehicle to achieve clear and simplified implementation of security policies. The untrust zone hosts the interfaces that have access to the Internet.

Figure 3 on page 7 shows the interfaces in each security zone.

Figure 3: Security Zones



The internal interfaces in the corporate Intranet are in the trust zone. Table 1 on page 7 shows the desired behavior of the security policies for traffic between zones.

Table 1: Security Policies by Zone

From Zone	To Zone	Security Policy Behavior
Trust	Trust	Yes
Untrust	Untrust	No
Trust	Untrust	Yes
Untrust	Trust	Trust-initiated only

Table 2 on page 8 summarizes the VLAN information and the IP address information for the interfaces.

Table 2: Interfaces Configuration Details

Interface	VLAN	IP Address	Network Mask
dl.0	-	DHCP	-
ge-0/0/7	-	DHCP	-
irb.0	3	192.0.2.1	255.255.255.0

Baseline Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

The steps in this configuration logically build from the lower layers to the upper layers.

1. After saving your existing configuration, delete it to start fresh for this example.

```
[edit ]
save backup
delete  This will delete the entire configuration Delete everything under this level?
[yes,no] (no)
yes
```

2. Assign a strong root password. The one shown below is for documentation purposes only!

```
[edit ]
set system root-authentication plain-text-password
New password: Enter_a_strong_root_password_h3re
Retype new password: Enter_a_strong_root_password_h3re
```

3. Copy and paste the below baseline configuration commands into a text editor and modify as needed to suit your environment. Load your edited commands into the CLI using the load set terminal configuration mode command.

```
[edit]
set system name-server 8.8.8.8
set system ntp server 216.239.35.12
set system time-zone America/Los_Angeles
set system syslog archive size 100k
set system syslog archive files 3
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file LOG-Accepted-Traffic any any
set system syslog file LOG-Accepted-Traffic match RT_FLOW_SESSION_CREATE
set system syslog file LOG-Accepted-Traffic archive size 1m
set system syslog file LOG-Accepted-Traffic archive files 3
set system syslog file LOG-Blocked-Traffic any any
set system syslog file LOG-Blocked-Traffic match RT_FLOW_SESSION_DENY
set system syslog file LOG-Blocked-Traffic archive size 1m
set system syslog file LOG-Blocked-Traffic archive files 3
set system syslog file LOG-Sessions any any
set system syslog file LOG-Sessions match RT_FLOW
set system syslog file LOG-Sessions archive size 1m
set system syslog file LOG-Sessions archive files 3
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 policies from-zone trust to-zone trust policy trust-to-trust match source-
address any
set security policies from-zone trust to-zone trust policy trust-to-trust match destination-
address any
set security policies from-zone trust to-zone trust policy trust-to-trust match application
any
```

```
set security policies from-zone trust to-zone trust policy trust-to-trust then permit
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 untrust interfaces dl0.0
set interfaces cl-1/0/0 dialer-options pool 1 priority 100
set interfaces dl0 unit 0 family inet negotiate-address
set interfaces dl0 unit 0 family inet6 negotiate-address
set interfaces dl0 unit 0 dialer-options pool 1
set protocols l2-learning global-mode switching
```

4. Commit the baseline configuration.

> **TIP**: When making changes to system authentication or to management access, consider using `commit confirmed`. The configuration will automatically roll back restoring remote access if your changes unexpectedly result in isolating you from the device.

```
[edit]
commit
```

Example Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

The steps in this configuration logically build from the lower layers to the upper layers.

1. Create a common VLAN for the LAN segment of the network. You also configure the irb interface and associate it with the VLAN.

```
[edit ]
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface irb.0
set interfaces irb.0 family inet address 192.0.2.1/24
```

2. Create a security policy that allows traffic between the trust and untrust zones. Make sure that you include the desired network segments and applications in the policy. You also add the trust VLAN subnet to the global address book. The named address is then referenced in the security policy.

```
[edit security]
set address-book global address vlan 192.0.2.0/24
set policies from-zone trust to-zone untrust policy allow-in-zone match source-address vlan
set policies from-zone trust to-zone untrust policy allow-in-zone match destination-address
any
set policies from-zone trust to-zone untrust policy allow-in-zone match application any
set policies from-zone trust to-zone untrust policy allow-in-zone then permit application-
services application-traffic-control rule-set critical_app_rs
```

3. Create a security policy that allows traffic between devices in the trust zone. Make sure that you include the desired network segments and applications in the policy.

```
[edit security]
set policies from-zone trust to-zone trust policy allow-in-zone match source-address vlan
set policies from-zone trust to-zone trust policy allow-in-zone match destination-address
vlan
set policies from-zone trust to-zone trust policy allow-in-zone match application any
set policies from-zone trust to-zone trust policy allow-in-zone then permit
```

4. Create a unique DHCP server group for the devices that are connected on the LAN segment.

```
[edit system]
set services dhcp-local-server group junosDHCPPool interface irb.0
```

5. Create a pool of IP addresses to be assigned to the devices that are in the LAN segment. Set the lowest and the highest IP addresses to be assigned to devices from this pool, the DNS servers, and the IP address of the default gateway for the pool that is the IP address of the `irb.0` interface.

```
[edit access]
set address-assignment pool junosDHCPPool family inet network 192.0.2.0/24
set address-assignment pool junosDHCPPool family inet range junosRange low 192.0.2.10
set address-assignment pool junosDHCPPool family inet range junosRange high 192.0.2.240
set address-assignment pool junosDHCPPool family inet dhcp-attributes name-server
198.51.100.0
set address-assignment pool junosDHCPPool family inet dhcp-attributes name-server
203.0.113.0
set address-assignment pool junosDHCPPool family inet dhcp-attributes propagate-settings
ge-0/0/7
set address-assignment pool junosDHCPPool family inet dhcp-attributes router 192.0.2.1
```

6. Create source NAT to apply NAT to devices in the trust zone to the outer interface. For more information about source NAT, see *Source NAT*.

```
[edit security]
set nat source rule-set trust-to-untrust from zone trust
set nat source rule-set trust-to-untrust to zone untrust
set nat source rule-set trust-to-untrust rule source-nat-rule match source-address
192.0.2.0/24
set nat source rule-set trust-to-untrust rule source-nat-rule then source-nat interface
```

7. Configure the primary interface.

```
[edit interfaces]
set ge-0/0/7 unit 0 description "WAN Interface 1 - Primary"
set ge-0/0/7 unit 0 family inet dhcp vendor-id Juniper-srx320
set ge-0/0/7 unit 0 backup-options interface dl0.0
```

8. Configure the modem (LTE-MPIM) interface.

```
[edit interfaces]
set cl-1/0/0 description “WAN Interfaces 2 – Backup”
set cl-1/0/0 dialer-options pool 1 priority 100
```

```
set cl-1/0/0 act-sim 1
set cl-1/0/0 cellular-options sim 1 radio-access automatic
```

9. Configure the dialer interface.

```
[edit interfaces]
set dl0 unit 0 family inet negotiate-address
set dl0 unit 0 family inet6 negotiate-address
set dl0 unit 0 dialer-options pool 1
set dl0 unit 0 dialer-options dial-string "*99#"
```

10. Configure the LAN interfaces ge-0/0/0, ge-0/0/1, and the others to be switching interfaces in the trust VLAN. The trust VLAN will effectively make them part of the trust zone. The configuration example shown is for one interfaces, specifically ge-0/0/0. Repeat the same steps for all LAN segment interfaces.

```
[edit interfaces]
set ge-0/0/0 unit 0 family ethernet-switching vlan members vlan-trust
```

11. Make sure that the necessary protocols are allowed in the trust zone. That ensures proper operation of the LAN segment of the network.

```
[edit security]
set zones security-zone trust host-inbound-traffic system-services all
set zones security-zone trust host-inbound-traffic protocols all
set zones security-zone trust interfaces irb.0
```

12. Ensure that the protocols are allowed in the untrust zone.

```
[edit security]
set zones security-zone untrust interfaces ge-0/0/7.0 host-inbound-traffic system-services
dhcp
set zones security-zone untrust interfaces ge-0/0/7.0 host-inbound-traffic system-services
tftp
set zones security-zone untrust interfaces ge-0/0/7.0 host-inbound-traffic system-services
netconf
set zones security-zone untrust interfaces dl0.0 host-inbound-traffic system-services tftp
```

13. Configure class of service, assign best-effort traffic to queue 0, and define rate limiters.

    The SRX320 devices support eight priority queues per interface for integrated Class of Service (CoS). Business-critical traffic is routed over `queue 0`.

```
[edit class-of-service]
set forwarding-classes queue 0 fc-class1
set application-traffic-control rate-limiters rate-limit-mb bandwidth-limit 1000
set application-traffic-control rate-limiters rate-limit-mb burst-size-limit 13000
```

14. Define AppQos rules and application match criteria.

    An AppQoS rule-set steers traffic through different queues. The first rule, `rule1`, steers the business-critical applications toward `queue 0` and sets low probability to drop traffic in case of congestion. The `restrule` rule enforces the shaper for the rest of the traffic in both directions (uplink and downlink). Salesforce and Office365 are identified as critical applications in this example.

```
[edit class-of-service application-traffic-control]
set rule-sets critical_app_rs rule rule1 match application [ junos:SALESFORCE
junos:OFFICE365 ]
set rule-sets critical_app_rs rule rule1 then forwarding-class fc-class1
set rule-sets critical_app_rs rule rule1 then loss-priority low
set rule-sets critical_app_rs rule restrule match application-any
set rule-sets critical_app_rs rule restrule then loss-priority high
set rule-sets critical_app_rs rule restrule rate-limit client-to-server then rate-limit-mb
set rule-sets critical_app_rs rule restrule rate-limit server-to-client then rate-limit-mb
```

15. Commit the configuration.

```
[edit]
commit
```

16. Set the Access Point Name for the SIM in the modem (LTE-MPIM).

NOTE: This is an operational mode command.

```
root@device>request modem wireless create-profile profile-id 10 access-point-name broadband
cl-1/0/0 slot 1
```

Results

The full configuration is provided in set format for reference:

```
set system root-authentication encrypted-password "$6$QkCmOYcl$cJZHOqj5F5AfSiJvXyTx8ewMkb4H/
Vw1yuHcJivgmQAAZRTOh/iUt/Glnwsdu8puPNAHeP8gYefnWFHo3UxL11"
set system services dhcp-local-server group junosDHCPPool interface irb.0
set system time-zone America/Los_Angeles
set system name-server 8.8.8.8
set system syslog archive size 100k
set system syslog archive files 3
set system syslog user * any emergency
set system syslog file LOG-Accepted-Traffic any any
set system syslog file LOG-Accepted-Traffic match RT_FLOW_SESSION_CREATE
set system syslog file LOG-Accepted-Traffic archive size 1m
set system syslog file LOG-Accepted-Traffic archive files 3
set system syslog file LOG-Blocked-Traffic any any
set system syslog file LOG-Blocked-Traffic match RT_FLOW_SESSION_DENY
set system syslog file LOG-Blocked-Traffic archive size 1m
set system syslog file LOG-Blocked-Traffic archive files 3
set system syslog file LOG-Sessions any any
set system syslog file LOG-Sessions match RT_FLOW
set system syslog file LOG-Sessions archive size 1m
set system syslog file LOG-Sessions archive files 3
set system syslog file messages any notice
set system syslog file messages authorization info
set system ntp server 216.239.35.12
set security address-book global address vlan 192.0.2.0/24
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
192.0.2.0/24
```

```
set security nat source rule-set trust-to-untrust rule source-nat-rule then source-nat interface
set security policies from-zone trust to-zone trust policy trust-to-trust match source-address
any
set security policies from-zone trust to-zone trust policy trust-to-trust match destination-
address any
set security policies from-zone trust to-zone trust policy trust-to-trust match application any
set security policies from-zone trust to-zone trust policy trust-to-trust then permit
set security policies from-zone trust to-zone trust policy allow-in-zone match source-address
vlan
set security policies from-zone trust to-zone trust policy allow-in-zone match destination-
address vlan
set security policies from-zone trust to-zone trust policy allow-in-zone match application any
set security policies from-zone trust to-zone trust policy allow-in-zone then permit
set security policies from-zone trust to-zone untrust policy allow-in-zone match source-address
vlan
set security policies from-zone trust to-zone untrust policy allow-in-zone match destination-
address any
set security policies from-zone trust to-zone untrust policy allow-in-zone match application any
set security policies from-zone trust to-zone untrust policy allow-in-zone then permit
application-services application-traffic-control rule-set critical_app_rs
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 irb.0
set security zones security-zone untrust interfaces dl0.0 host-inbound-traffic system-services
tftp
set security zones security-zone untrust interfaces ge-0/0/7.0 host-inbound-traffic system-
services dhcp
set security zones security-zone untrust interfaces ge-0/0/7.0 host-inbound-traffic system-
services tftp
set security zones security-zone untrust interfaces ge-0/0/7.0 host-inbound-traffic system-
services netconf
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/7 unit 0 description "WAN Interface 1 - Primary"
set interfaces ge-0/0/7 unit 0 family inet dhcp vendor-id Juniper-srx320
set interfaces ge-0/0/7 unit 0 backup-options interface dl0.0
set interfaces cl-1/0/0 description "“WAN"
set interfaces cl-1/0/0 dialer-options pool 1 priority 100
set interfaces cl-1/0/0 act-sim 1
set interfaces cl-1/0/0 cellular-options sim 1 radio-access automatic
set interfaces dl0 unit 0 family inet negotiate-address
set interfaces dl0 unit 0 family inet6 negotiate-address
set interfaces dl0 unit 0 dialer-options pool 1
set interfaces dl0 unit 0 dialer-options dial-string "*99#"
```

```
set interfaces irb unit 0 family inet address 192.0.2.1/24
set class-of-service forwarding-classes queue 0 fc-class1
set class-of-service application-traffic-control rate-limiters rate-limit-mb bandwidth-limit 1000
set class-of-service application-traffic-control rate-limiters rate-limit-mb burst-size-limit
13000
set class-of-service application-traffic-control rule-sets critical_app_rs rule rule1 match
application junos:SALESFORCE
set class-of-service application-traffic-control rule-sets critical_app_rs rule rule1 match
application junos:OFFICE365
set class-of-service application-traffic-control rule-sets critical_app_rs rule rule1 then
forwarding-class fc-class1
set class-of-service application-traffic-control rule-sets critical_app_rs rule rule1 then loss-
priority low
set class-of-service application-traffic-control rule-sets critical_app_rs rule restrule match
application-any
set class-of-service application-traffic-control rule-sets critical_app_rs rule restrule then
loss-priority high
set class-of-service application-traffic-control rule-sets critical_app_rs rule restrule then
rate-limit client-to-server rate-limit-mb
set class-of-service application-traffic-control rule-sets critical_app_rs rule restrule then
rate-limit server-to-client rate-limit-mb
set access address-assignment pool junosDHCPPool family inet network 192.0.2.0/24
set access address-assignment pool junosDHCPPool family inet range junosRange low 192.0.2.10
set access address-assignment pool junosDHCPPool family inet range junosRange high 192.0.2.240
set access address-assignment pool junosDHCPPool family inet dhcp-attributes name-server
198.51.100.0
set access address-assignment pool junosDHCPPool family inet dhcp-attributes name-server
203.0.113.0
set access address-assignment pool junosDHCPPool family inet dhcp-attributes router 192.0.2.1
set access address-assignment pool junosDHCPPool family inet dhcp-attributes propagate-settings
ge-0/0/7
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface irb.0
set protocols l2-learning global-mode switching
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform this task:

Verifying the Mini-PIM modules detected by Junos OS.

Purpose

Verifying the Mini-PIM modules detected by Junos OS.

Action

From operational mode:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                CX0916AF0004      SRX320-POE
Routing Engine   REV 0x05 650-065041   CX0916AF0004      RE-SRX320-POE
FPC 0                                                    FPC
  PIC 0                                                  6xGE,2xGE SFP Base PIC
FPC 1            REV 02   650-073958   AH06074206        FPC
  PIC 0                                                  LTE for AE
Power Supply 0
```

Meaning

The output lists the Mini-PIM modules detected. The Mini-PIM slot number is reported as an FPC number, and the Mini-PIM number (always 0) is reported as the PIC number.

Verifying the Firmware Version of the Mini-PIMs

Purpose

Verify the firmware version of the Mini-PIMs.

Action

From operational mode:

```
user@host> show system firmware

Part             Type              Tag  Current              Available           Status
                                        version              version
FPC 1
PIC 0            MLTE_FW           1    17.1.80             0                    OK
Routing Engine 0 RE BIOS           0    3.0                  3.6                  OK
Routing Engine 0 RE BIOS Backup    1    3.0                  3.6                  OK
```

Meaning

The output shows the firmware version of the Mini-PIM as 17.1.80.

Verifying the Traffic on the WAN Interface

Purpose

Verify the traffic is passing through the expected queue on the WAN interface.

Action

From operational mode:

```
user@host> show interfaces ge-0/0/7 extensive
Physical interface: ge-0/0/7, Enabled, Physical link is Up
  Interface index: 136, SNMP ifIndex: 513, Generation: 139
  Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,
  BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled,
```

```
Remote fault: Online
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x0
Link flags     : None
CoS queues     : 8 supported, 8 maximum usable queues
Hold-times     : Up 0 ms, Down 0 ms
Current address: 64:64:9b:05:8b:26, Hardware address: 64:64:9b:05:8b:26
Last flapped   : 2020-04-09 15:46:13 PDT (4w3d 00:58 ago)
Statistics last cleared: Never
Traffic statistics:
 Input  bytes  :             33066002                   0 bps
 Output bytes  :                    0                   0 bps
 Input  packets:               104182                   0 pps
 Output packets:                    0                   0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 260770, L2 mismatch timeouts: 0,
  FIFO errors: 0, Resource errors: 0
Output errors:
  Carrier transitions: 5, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
  FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters:       Queued packets  Transmitted packets      Dropped packets
  0 best-effort                    0                    0                    0
  1 expedited-fo                   0                    0                    0
  2 assured-forw                   0                    0                    0
  3 network-cont                   0                    0                    0
Queue number:         Mapped forwarding classes
  0                   best-effort
  1                   expedited-forwarding
  2                   assured-forwarding
 3                   network-control
```

Meaning

The output shows that the best-effort, expedited-forwarding, assured-forwarding, and network-control traffic is passing through expected queues 0, 1, 2, and 3, respectively on the WAN interface.